Universidad Carlos III de Madrid

Escuela Politécnica Superior

Departamento Tecnología Electrónica

Ingeniería Técnica de Telecomunicación: Sonido e Imagen

Proyecto Fin de Carrera

Evaluación Biométrica de Algoritmos de Autenticación de Firma Manuscrita

Autor: María Antonia Ávila Jiménez

Director: Óscar Miguel Hurtado

Leganés, 2010

Proyecto Fin de Carrera

Evaluación Biométrica de Algoritmos de Autenticación de Firma Manuscrita

AUTOR: **María Antonia Ávila Jiménez**

Tutor: **Óscar Miguel Hurtado**

TRIBUNAL CALIFICADOR

PRESIDENTE: Raúl Sánchez Reillo

SECRETARIO: Luis Mengibar Pozo

VOCAL: Matilde Pilar Sánchez Fernández

CALIFICACIÓN:

Leganés, a de de 2010

Agradecimientos

La realización del Proyecto Fin de Carrera es una labor que requiere mucho trabajo, sacrificio y dedicación. Por unos motivos u otros, a pesar de toda la de dedicación y atención que he puesto en este trabajo, ha habido muchas pausas y periodos de inactividad, debido a ciertos problemas, que me han enseñado lo que cuesta retomar un proyecto, y han provocado que su realización se extienda más de lo que a cualquiera le gustaría.

Sin embargo, una vez terminado y con el duro trabajo de todos estos meses, sobre todo estos últimos, materializado en un libro, puedo decir que ha merecido la pena. Ha merecido la pena porque he aprendido mucho, no solo sobre el tema acerca del que versa el proyecto, la programación que lleva a cabo, sino también sobre lo importante que es tener cerca a personas que te apoyen durante el trayecto, especialmente en los momentos difíciles.

Es por eso que quiero dedicar este trabajo a todas aquellas personas que, de una manera u otra, me han acompañado en este largo camino. Muchas han caminado conmigo de principio a fin, y otras solo en algunos tramos. De cualquier manera, si he seguido adelante en todo momento ha sido gracias a todos ellos, y por eso parte de este proyecto les pertenece.

En primer lugar, quiero dar las gracias a mi familia. Todos y cada uno de ellos se han volcado con este trabajo, y siempre han estado pendientes de los avances dándome todo su apoyo. En especial, quiero agradecérselo a mis padres, ya que siempre han confiado en mí y me han enseñado que nunca y en ningún momento se puede dar nadie por vencido, que para todo hay remedio excepto para la muerte y siempre hay que buscar lo positivo de las cosas.

También quiero dar las gracias dos personas muy especiales e importantes en mi vida, a mi hermana y a mi novio, que me han mostrado cual es el camino a seguir y me han apoyado incondicionalmente, como nadie lo ha hecho. A pesar del hundimiento, lágrimas... siempre estabais cerca y animándome para seguir adelante.

A mis niñas, Cristina, Ana Belén y Tamara, gracias por estar a mi lado a lo largo de todos estos años y de haberme dado la oportunidad de conoceros y saber lo mucho que valéis cada una de vosotras.

A Rosa, gracias por todo lo que has hecho por mí. Gracias por tu apoyo y seguimiento durante este tiempo. Has sido como una tutora para mí, una gran amiga, has sido... no hay palabras que describan todo lo que siento, para expresarte lo agradecida que estoy de haberte tenido a mi lado. Muchas gracias.

Por último, quiero darle las gracias a mi tutor, por haberme dado la oportunidad de realizar este proyecto del cual me siento muy orgullosa.

Resumen

El papel continúa siendo el medio más utilizado por todos nosotros para acompañar y transmitir la información, aún a pesar de las nuevas tecnologías. No obstante, los procesos de digitalización se están acercando rápidamente a las empresas. Actualmente, muchas de ellas, han decidido reducir drásticamente el flujo de papel a través de la digitalización, a pesar de su elevado coste y su impacto negativo en la productividad del empleado. Pero ciertos documentos, en los cuales existe una firma manuscrita, suelen quedar fuera de este proceso de digitalización. El motivo se debe, a que la digitalización de la firma, históricamente ha carecido de apoyo jurídico y legal, por lo que obliga a las empresas a seguir manteniendo sus documentos y transacciones en formato papel.

La aparición de la nueva ley que regula de forma definitiva la firma digital o electrónica, abre multitud de puertas para favorecer esa nueva corriente de digitalización.

El alcance de este proyecto se centra en el estudio, y evaluación de tres algoritmos: GMM(Modelo de Mezcla de Gaussianas), DTW (Dynamic Time Warping) y DTW+GMM(mezcla de los dos algoritmos anteriores), con el fin de obtener las tasas de error para verificar si una firma es verdadera o falsa.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

En este capítulo se describe el contexto en el que se ha desarrollado el presente trabajo: Evaluación biométrica de algoritmos de autentificación de firma manuscrita. A continuación se concretan las motivaciones que promueven el trabajo aquí presentado así como los resultados que se esperan obtener. Esta introducción se cierra con un breve resumen del contenido de cada uno de los capítulos, que trata de dar una visión global del trabajo realizado.

1.1 Contexto

El contexto tecnológico de la palabra biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características corporales o de comportamiento de las personas con el objeto de establecer una identidad. Para diferenciar estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autentificación biométrica.

La biometría busca la automatización de tareas que involucran el reconocimien-

to o autentificación de la identidad de usuario.

1.2 Motivación

El creciente desarrollo y utilización de potentes terminales como Tablet PC o PDAs así como la proliferación de redes de comunicaciones de banda ancha, posibilitan el uso de sistemas automáticos para el reconocimiento y verificación automático de usuarios mediante diversos rasgos biométricos en el que se encuentra la firma manuscrita.

La seguridad que proporciona el uso de rasgos biométricos es muy superior frente a los sistemas actuales (claves, DNI ...) al no poder ser robados, perdidos u olvidados. En entornos de seguridad crítica (bancarios, militar ...) el valor añadido que aportan estos sistemas automáticos es enorme.

La firma manuscrita es uno de los medios de verificación de identidad por excelencia, lo que ha proporcionado que haya sido objeto de muchas y diversas líneas de investigación. La seguridad, aceptación y arraigo de la firma como medio de autentificación personal, social y legal, confieren enormes posibilidades de futuro a este trabajo especialmente en ámbitos donde la seguridad sea parte fundamental de su actividad.

En este entorno, queremos evaluar cómo las características de captura de estos nuevos productos tanto de alto coste como bajo coste, pueden afectar al rendimiento de los algoritmos de autentificación de firma manuscrita.

Para ello se desarrollará un protocolo de evaluación, basado en la norma internacional ISO/IEC 19795 "Biometric performance testing and reporting"[MWD+02], [ISO05], [ISO06], y una vez realizada la misma, evaluar el impacto que tienen sobre el rendimiento de los algoritmos las distintas características de los dispositivos de de captura.

Por otro lado, se estudiará como influyen las características de la firma del usuario en el rendimiento de los algoritmos. Dichas características son las definidas en el anexo B de la norma ISO/IEC 19794-11 "Signature/Sign Processed Dynamic Data"[ISO09].

1.3 Objetivos

El objetivo fundamental de este proyecto es la generación de un método de evaluación de algoritmos de firma basado en la norma 19795[MWD+02] y una vez creado dicho método, aplicarlo para el estudio de la influencia de la resolución en la captura de la firma. Esta captura está basada en diferentes aspectos a tener en cuenta que serán nuestro objeto de estudio, como son la resolución en las coordenadas X e Y, es decir, las coordenadas del dispositivo donde firma el usuario, la resolución en la presión, con qué fuerza presiona el usuario el dispositivo al firmar y la resolución en la frecuencia de muestreo.

El proyecto se va a dividir en tres grandes bloques: creación de un método de evaluación conforme a la norma citada anteriormente, evaluación de la influencia de la resolución en X,Y,P y T para tres algoritmos de firma manuscrita DTW[SC78], GMM[O. 07b], y DTW+GMM[O. 07a], los cuales serán descritos posteriormente, y por último el estudio del Anexo B de la norma 19794-11[ISO09].

1.4 Organización del Documento

- **Capítulo 1**:En este capítulo se describe el contexto en el que se ha desarrollado el presente trabajo: Evaluación biomtrica de algoritmos de autentificación de firma manuscrita. A continuación se concretan las motivaciones que promueven el trabajo aquí presentado así como los resultados que se esperan obtener. Esta introducción se cierra con un breve resumen del contenido de cada uno de los capítulos, que trata de dar una visión global del trabajo realizado.

- **Capítulo 2**: En este capítulo se realiza una revisión del estado actual de la investigación en la biometría centrándose en el área en el que vamos a trabajar, la firma manuscrita. El estudio se particulariza sobre los aspectos que tienen mayor incidencia en el desarrollo de este proyecto. En este sentido, se estudian con mayor detalle dos aplicaciones potenciales de los sistemas de evaluación biométrica: sistemas basados en alineamiento temporal dinámico (DTW) y

sistemas de modelo de mezclas gaussianas (GMM).

- **Capítulo 3**: En este capítulo nos centraremos en lo que es en sí nuestro objeto de evaluación, es decir, conoceremos a fondo el significado de una firma, su origen, los componentes que posee así como el procedimiento a seguir para su reconocimiento a la hora de hacer una evaluación. Por otro lado expondremos los parámetros a estudiar junto con los algoritmos que nos ayudarán en el estudio.

- **Capítulo 4**: En este capítulo nos centraremos en describir cómo se ha diseñado, qué forma tiene y cómo funciona nuestro proyecto.

- **Capítulo 5**: En este capítulo presentamos los resultados de las evaluaciones para cada uno de los algoritmos que hemos descrito en el capítulo 3, GMM, DTW y DTW+GMM. Los resultados se dividen en varias partes, en la primera se analizará cada uno de ellos sin realizar ningún escalado a la base de datos, luego evaluaremos los algoritmos escalando las firmas para ver como afecta este escalado al rendimiento de los algoritmos. En la última parte analizaremos los tres aspectos indicados en el anexo B de la norma internacional ISO/IEC 19794-11 como indicadores del nivel de seguridad en la firma de un usuario.

- **Capítulo 6**: En este capítulo nos centraremos en expresar las conclusiones a las que hemos llegado al obtener los resultados y los posibles trabajos futuros.

- **Bibliografía**

Capítulo 2

Estado del Arte

En este capítulo se realiza una revisión del estado actual de la investigación en la biometría centrándose en el área en el que vamos a trabajar, la firma manuscrita. El estudio se particulariza sobre los aspectos que tienen mayor incidencia en el desarrollo de este proyecto. En este sentido, se estudian con mayor detalle dos aplicaciones potenciales de los sistemas de evaluación biomítrica: sistemas basados en alineamiento temporal dinámico (DTW) y sistemas de modelo de mezclas gaussianas (GMM).

2.1 ¿Qué es la biometría?

Según la Real Academia Española, se define la biometría como el estudio mensurativo o estadístico de los fenómenos o procesos biológicos. Si estudiamos su significado etimológico, la biometría proviene del griego, siendo la suma de dos conceptos: "bios" que significa "vida" y "metron" cuyo significado es "medida".

Sin embargo, la biometría también se emplea para referirse a los métodos automáticos usados para analizar diferentes características humanas con el fin de identificar y autentificar a las personas.

Al referirse al término Biometría dentro del campo de Identificación de personas,

la definición se hace mas específica. Se podría decir, en este último caso, que la biometría es un sistema automatizado de reconocimiento humano basado en las características físicas y/o de comportamiento de las personas. Es el mismo sistema que utiliza el cerebro humano para reconocer y distinguir una persona de la otra. Este sistema, reconoce a la persona fijándose en " quién " es la persona, no importando "lo que la persona esté llevando" o "lo que la persona conoce". Objetos que una persona puede llevar, así como llaves y tarjetas de identificación, pueden ser perdidas, sustraídas y/o duplicadas. Datos que una persona conoce, tales como contraseñas y códigos, pueden ser olvidadas, sustraídas y/o duplicadas. Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de ambas.

Por tanto podemos concluir que la biometría es un método automatizado empleado para la identificación o autentificación de individuos mediante el estudio de ciertas características físicas y/o del comportamiento de las personas.

Debido a ello, esta técnica se basa en la captura de datos acerca de rasgos distintivos de un individuo (huella dactilar, voz, iris, firma manuscrita) para así poder compararla con otras muestras obtenidas anteriormente o pertenecientes a otros sujetos.

Hoy en día es palpable el rechazo que produce en amplios sectores de la sociedad el acceso a nuevos servicios, como el comercio electrónico, por la carencia de procedimientos fiables que permitan la identificación segura del usuario que accede al servicio. El nivel de seguridad que proporcionan las técnicas clásicas basadas en la posesión de un objeto (tarjeta) o una información (número personal), se ve ampliamente superado por nuevas técnicas que trabajan a partir de rasgos personales cuantificables.

De esta forma se puede obtener la identidad de una persona a partir de lo que es, y no a partir de lo que posee (tarjeta, llave) o lo que conoce (claves).

En la actualidad los dispositivos biométricos utilizan, entre otros rasgos, las huellas dactilares, la firma escrita, la cara o la voz para reconocer la identidad de una persona. Sin embargo, cada vez más se está investigando en nuevos algoritmos y técnicas que nos permitan implementar sistemas multimodales que combinen varios de estos rasgos característicos de la persona para obtener una identificación más fiable y segura.

Por otra parte, el desarrollo de estándares industriales de interoperabilidad biométrica, el desarrollo de sistemas de reconocimiento a gran escala sobre amplias poblaciones de usuarios y el empleo de información biométrica integrada sobre tarjeta inteligente permiten asegurar el éxito, tanto desde el punto de vista tecnológico como desde el coste económico asociado, con vistas a la incorporación de tecnología biométrica en aplicaciones reales.

2.2 Identificación y Autentificación

Los sistemas que los seres vivos usamos para identificar a una persona, son demasiado complejos. Debido a ello y desde el punto de vista del funcionamiento de los sistemas automáticos de reconocimiento de personas mediante rasgos biométricos, se hace necesario clasificar las dos perspectivas fundamentales de trabajo de los mismos:

- Sistemas de reconocimiento en modo identificación.
- Sistemas de reconocimiento en modo verificación.

2.2.1 Sistemas de reconocimiento en modo identificación

En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos. Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de este

proceso es la identidad del individuo, mientras que en la autentificación/verificación es un valor verdadero o falso. El gran inconveniente de este tipo de sistemas es que necesitan una base de datos para poder almacenar en ella todos los patrones tomados, así como una red de comunicaciones que permita la comunicación entre el sistema de almacenamiento de la información de los usuarios y cada uno de los puntos de reconocimiento.

La figura siguiente muestra de forma genérica la estructura típica de un sistema de identificación.

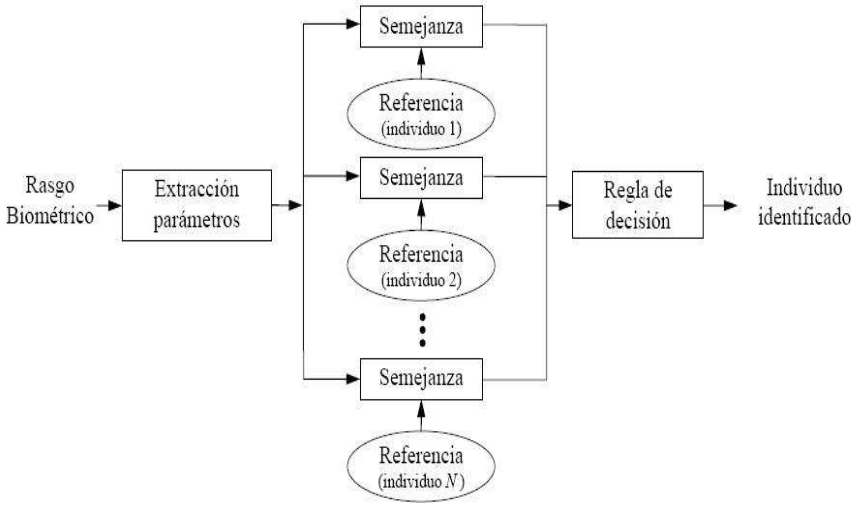


Figura 2.1: Estructura de un sistema de identificación.

Dentro de estos sistemas, debemos diferenciar dos posibles casos:

- *Identificación en conjunto cerrado*: en este caso, el resultado del proceso es una asignación de identidad a uno de los individuos modelados por el sistema, y conocidos como usuarios. Existen, por tanto, N posibles decisiones de salida posibles.

- *Identificación en conjunto abierto*: aquí debemos considerar una posibilidad adicional a las N del caso anterior: que el individuo que pretende ser identificado no pertenezca al grupo de usuarios, con lo que el sistema de identificación

debería contemplar la posibilidad de no clasificar la realización de entrada como perteneciente a las N posibles.

A continuación, en la figura 2.2, mostraremos un ejemplo de lo que hará un sistema de identificación.

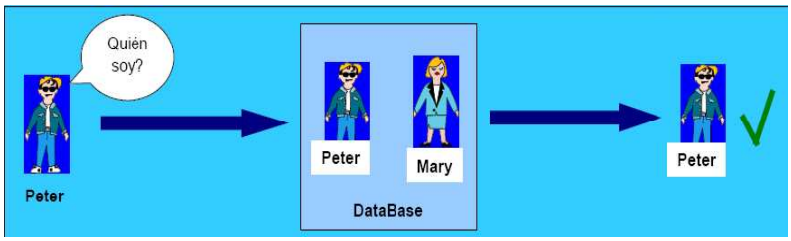


Figura 2.2: Ejemplo de identificación.

2.2.2 Sistemas de reconocimiento en modo verificación

Este tipo de sistemas se encarga de autentificar la identidad reclamada por el usuario, por lo que las muestras de este individuo sólo se compararan con el patrón perteneciente a la identidad de dicha persona. A partir del rasgo biométrico capturado al usuario y de la identidad proporcionada, el sistema es el que se encarga de decir si es o no cierto que pertenece a dicha persona. Un aspecto relevante es que el individuo deberá facilitar, aparte de su característica biométrica, algún tipo de identificador de su identidad. De este modo, las dos únicas salidas o decisiones del sistema son la aceptación o el rechazo del individuo como aquel que pretende ser. De esta forma, el locutor solicitante será catalogado como usuario auténtico o bien como impostor, respectivamente. La decisión de aceptar o rechazar la entrada como correspondiente al usuario solicitado dependerá de si el valor de parecido o probabilidad obtenido supera o no un determinado umbral de decisión.

El proceso de autentificación o verificación biométrica es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios es elevado. Esto es debido a que la necesidad de procesamiento y comparaciones es más reducida en el proceso de autentificación. Por esta razón, es habitual usar autentificación cuando

se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o se quiere un proceso muy rápido. Por otro lado, cabe destacar que se necesita fijar un umbral con el cual medir el grado de diferencia existente entre el vector de características y el patrón almacenado.

La figura siguiente,figura 2.3, muestra de forma genérica la estructura típica de un sistema de verificación.

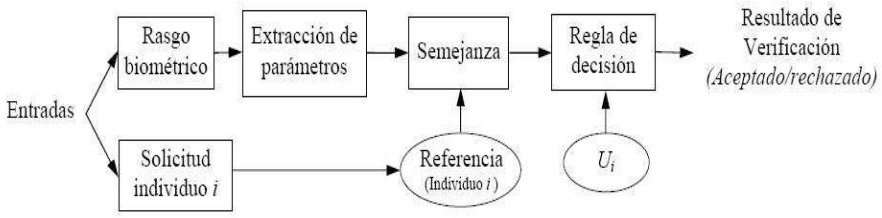


Figura 2.3: Estructura de un sistema de verificación.

A continuación, en la figuras 2.4, mostraremos un ejemplo de lo que haría un sistema de verificación.

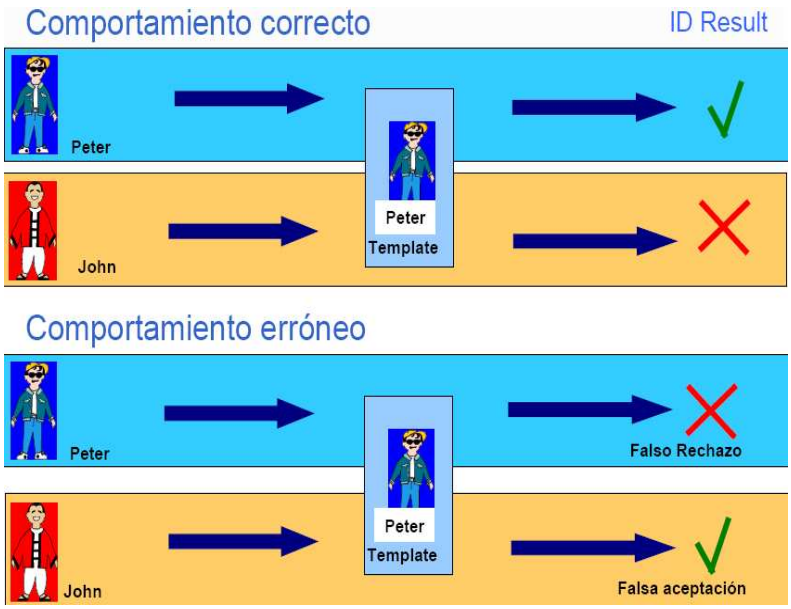


Figura 2.4: Ejemplo de un sistema de verificación.

2.3 Reconocimiento biométrico

Se denomina reconocimiento biométrico al proceso que permite asociar una identidad con un individuo de forma automática, mediante el uso de alguna característica personal física o del comportamiento que le sea inherente.

Aunque en el ámbito forense (judicial, policial y pericial), el análisis científico de evidencias biométricas se ha venido usando desde hace más de un siglo, el reconocimiento biométrico como medio automático de autenticación personal en aplicaciones comerciales o civiles es un área de investigación y desarrollo bastante más reciente.

Hoy en día el reconocimiento biométrico se puede considerar como un campo de investigación asentado con libros de referencia (Jain et al., 1999; Ratha and Bolle, 2004; Wayman et al., 2005), conferencias específicas en el tema (Kittler and Nixon, 2003; Maltoni and Jain, 2004; Jain and Ratha, 2004), evaluaciones y pruebas comparativas (Phillips et al., 2000; Grother et al., 2003; Przybocki and Martin, 2004; Wilson et al., 2004; Maio et al., 2004; Yeung et al., 2004), proyectos internacionales (COST-275, 2005; BioSec, 2004; Biosecure, 2004), consorcios (EBF, 2005; BC, 2005), esfuerzos de estandarización (BioAPI,2002; SC37, 2005), y un creciente interés tanto por parte de gobiernos (DoD, 2005) como del sector comercial (International Biometric Group, 2006).

Pese a la madurez de este campo de investigación, con trabajos que se remontan más de tres décadas en el tiempo (Kanade, 1973; Atal, 1976; Nagel and Rosenfeld, 1977), el reconocimiento biométrico sigue siendo un área muy activa de investigación, con numerosos problemas prácticos aún por solucionar (Jainet al., 2004a). Estos problemas prácticos han hecho que, pese al interés de las aplicaciones biométricas, la integración en el mercado de estas nuevas tecnologías sea más lenta de lo esperado.

Dentro del reconocimiento biométrico se pueden utilizar diferentes rasgos para identificar al usuario: huella dactilar, voz, iris, cara, firma, etc. Estos se pueden clasificar asimismo en patrones fisiológicos (huella, geometría de la mano, iris) y patrones de comportamiento (firma, voz, modo de teclear).

La conveniencia de uno u otro rasgo para determinada aplicación se estudia teniendo en cuenta:

- *Universalidad*: existencia del rasgo en todos los usuarios.
- *Unicidad*: capacidad discriminativa del rasgo (personas distintas deben poseer rasgos distintos).
- *Permanencia*: variabilidad del rasgo en el tiempo.
- *Mensurabilidad*: capacidad para caracterizar el rasgo cuantitativamente.
- *Aceptabilidad*: grado de aceptación personal y social.
- *Rendimiento*: precisión y rapidez en la identificación.
- *Evitabilidad*: capacidad de eludir/burlar el sistema.

Cada rasgo biométrico destaca en algún atributo y flaquea en otro, no existiendo uno solo que abarque todos con éxito. Existen dos tipos de métodos de reconocimiento (ver figura 2.5):

- *Colaborativo*: el usuario está informado de la presencia de un sistema biométrico. Es necesario que esté familiarizado con él. Debe decidir si usarlo o no.
- *No colaborativo*: el usuario no tiene que realizar ninguna acción. El sistema puede no ser detectado por el usuario. Resulta mucho más cómodo para el usuario. El sistema puede extraer características biométricas del usuario a distancia independientemente de su posición en el entorno.

Una forma de mejorar la fiabilidad del reconocimiento biométrico es utilizar distintos tipos de información biométrica al llevar a cabo la identificación. Esta modalidad se denomina multibiometría y se puede realizar a distintos niveles.

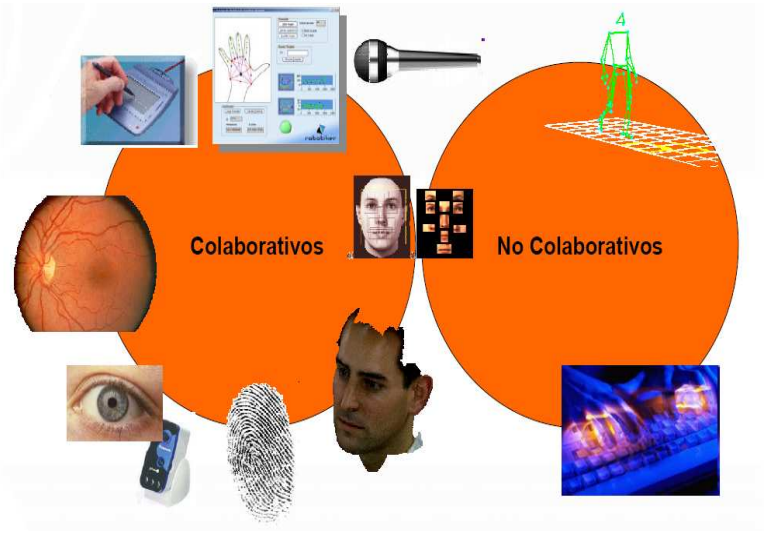


Figura 2.5: Métodos de reconocimientos.

2.4 Evaluación de un sistema biométrico

Los Sistemas de Identificación Biométrica tienen mucho que ver con la seguridad. Por un lado, el hecho de que se utilicen como medio seguro de autenticación, y por otro, el utilizar datos muy sensibles, debe requerir un análisis completo sobre la seguridad del sistema.

La mayoría de las veces se relaciona la biometría con la seguridad, pero desafortunadamente, muy poco se ha hecho al respecto. Se ha trabajado mucho a la hora de evaluar el rendimiento funcional de un sistema biométrico, fundamentalmente basándose en el análisis de las tasas de error, y en algunos casos, relacionándolas con consumos, tamaño de código, tiempo de procesamiento, etc. Desde un punto de vista más formal, ISO ha iniciado una serie de normas (ISO/IEC 19795)[MWD+02],[ISO05],[ISO06] relacionado con la evaluación del rendimiento de los sistemas biométricos, basándose, fundamentalmente, en las experiencias y trabajos realizados.

Estos trabajos se consideran de una gran valía para evaluar la seguridad en biometría, ya que el rendimiento y, especialmente, las tasas de error, tienen un impacto real en el grado de seguridad alcanzable.

La evaluación que se llevará a cabo en este proyecto a la hora de evaluar nues-

tro sistema estará centrada en la norma ISO / IEC 19795 [MWD+02]. En ella se establecen los requisitos y recomendaciones sobre la recopilación de datos, análisis y presentación de informes específicos para tres técnicas principales en la evaluación: evaluación tecnológica, evaluación del escenario y evaluación funcional que posteriormente serán explicadas ampliamente cada una de ellas.

Por otro lado, se encargará de presentar los requisitos y las mejoras para el desarrollo de pruebas para observar el rendimiento del sistema, así como proporcionará el asesoramiento específico para el desarrollo y utilización de los diferentes protocolos de ensayo.

La evaluación de un sistema biométrico implicará la recopilación de muestras o datos de entrada, que se utilizan para la generación de plantilla o patrón en el alistamiento, y para el cálculo de los resultados. Las muestras recogidas pueden ser utilizadas en el momento de la captura (online/en línea) inmediatamente para alistar en línea o un intento de identificación, o puede ser almacenadas y utilizadas más tarde (offline/fuera de línea).
Por tanto, podemos tener dos formas de evaluación:

- *Evaluación Online/En línea*: Son aquellas evaluaciones en las cuales el alistamiento o la comparación se realiza en el momento de capturar la muestra biométrica. Esto tiene la ventaja de que la muestra biométrica puede ser descartada de inmediato, por lo que nos ahorramos el proceso de almacenamiento y permitiremos que el sistema opere de una manera diferente a lo habitual. Sin embargo, se recomienda que se recojan todas las muestras, siempre que sea posible.

  Requiere de menos memoria y capacidad que el anlisis que mencionaremos posteriormente.

- Evaluación Offline/Fuera de línea:

  Son aquellas evaluaciones en las cuales tanto la inscripción como la clasificación de las muestras, se realizan con muestras adquiridas previamente.

  El hecho de poder tener previamente una base de datos para poder realizar la

inscripción fuera de línea, provoca que tengamos un mayor control sobre los intentos y los patrones que podrán ser usados en cualquier momento.

Existen diferentes técnicas de evaluación: tecnológica, de escenario y operacional. Dependiendo de lo que se desee evaluar, se seleccionará una de ellas. A continuación se explicarán estos tres tipos de evaluación:

- *Evaluación Tecnológica*:

  El objetivo es comparar algoritmos de una sola tecnología. Las pruebas de todos los algoritmos se realizan sobre una base de datos (en nuestro caso una base de datos que contiene 100 usuarios con 25 firmas genuinas y 25 firmas falsas cada uno) normalizada, la cual, idealmente, se obtiene mediante un sensor "universal". Dicho sensor, recoge de igual modo las muestras para todos los algoritmos que vayan a ser probados. Sin embargo, los resultados dependerán del entorno en el que se hayan recogido los datos y la población en la que hayan sido recogidas.. Hay que tener en cuenta que las pruebas han de hacerse con datos que previamente no hayan sido vistos por los desarrolladores del algoritmo.

  Los ensayos realizados se hacen fuera de línea utilizando los datos de prueba recogidos. La base de datos es fija, por tanto los resultados de las pruebas de tecnología son repetibles.

  La utilidad de este tipo de evaluación se deriva de su separación entre persona humana e interacción de la misma y la adquisición de datos por sensores en el proceso de reconocimiento. Todo ello conlleva una serie de beneficios como pueden ser:

  - Plena capacidad de llevar a cabo pruebas de comparación cruzada
  - Capacidad para llevar a cabo pruebas exploratorias.
  - Capacidad para realizar pruebas multi-algoritmicas.

- *Evaluación de Escenario*: El objetivo es determinar el rendimiento global del sistema a través de un prototipo o aplicación simulada. La evaluación es lle-

vada a cabo con el sistema completo y en un entorno que modele o simule el entorno donde se usará realmente. Por lo tanto, cada sistema evaluado tendrá sus propios dispositivos de captura de muestras y recibirá los datos de manera diferente. En consecuencia, será necesario que la recopilación de datos, para la evaluación de los distintos sistemas completos, se haga en el mismo entorno y con la misma población. Dependiendo de la capacidad de almacenamiento de datos de cada uno de los dispositivos, las pruebas pueden ser una combinación de pruebas en línea y fuera de línea. Los resultados de la prueba serán repetibles sólo cuando el modelo escenario pueda ser controlado de manera muy cuidadosa.

La utilidad de este tipo de evaluación se deriva de la inclusión de la adquisición de los datos, interacción en el alistamiento y los procesos de reconocimiento. Todo ello conlleva unos beneficios de los que podemos destacar la capacidad para medir el impacto de los intentos y operaciones adicionales en la capacidad del sistema tanto para realizar el aislamiento de los usuarios, como para realizar la identificación/autentificación.

- *Evaluación Funcional u Operacional*:El objetivo es determinar el rendimiento de un sistema biométrico en un entorno de aplicación específico y con una población específica. Dependiendo de la capacidad de almacenamiento de datos del dispositivo de prueba, las pruebas fuera de línea podran no ser posibles. En general, los resultados de las pruebas de funcionamiento no serán repetibles por las diferencias (normalmente desconocidas o no documentadas) entre distintos entornos operativos.

Para tener claros los conceptos de los diferentes tipos de evaluación, vamos a establecer una comparación entre ellos mediante una tabla (ver tabla 2.1).

	Tecnología	Escenario	Operacional
¿Qué se prueba?	Componentes biométricos	Sistemas Biométricos	Componentes biométricos
Comportamiento de los usuarios	No aplicable durante la prueba, pueden ser controlados cuando los datos biométricos están registrados, sino se considerará no controlado	Controlado (excepto si los comportamientos de los usuarios son una variable independiente)	Incontrolado
Reacción de un usuario en tiempo real ante el resultado de un intento	No	Si	Si
Repetitividad de los resultados	Si	Cuasi-repetible (si el escenario y la población están controladas)	No repetible
Control físico del entorno	Puede ser controlado cuando el dato biométrico está grabado, de otro modo, se considerará incontrolado	Controlado y/o grabado	No controlado, idealmente grabado
Interacción de los usuarios registrados	No se aplica durante la prueba. Puede ser grabado cuando los datos biométricos son grabados	Grabado	Grabado durante la inscripción. Pueden ser registrados durante la verificación/identificación
¿Qué resultados se proporcionan?	Comparación de los datos, componentes. Determinación de los factores de rendimiento	Comparación de los sistemas biométricos, determinación de los factores de rendimiento. Mide el rendimiento operativo	Medición del rendimiento operativo del entorno
Medidas típicas	Rendimiento, tasas de error (buenas para el proceso de identificación del sistema donde existen dificultades en la recopilación de pruebas con población a gran escala)	Rendimiento, FMR, FMNR, FTA FTE, FAR, FRR	Rendimiento, las pruebas fiables de FAR y operativos TRF requieren un poco de conocimiento de las premisas de partida
Limitaciones	Pruebas con la BBDD	Operacional, sistema instrumentado	Operacional, sistema instrumentado
Pruebas de población humana	Grabada	En directo/En vivo	En directo/En vivo

Tabla 2.1: Diferencias entre los tipos de evaluación.

2.5 Modalidades Biométricas

Aunque las características de la huella dactilar son, sin lugar a duda, las más ampliamente utilizadas para realizar una identificación biométrica, cualquier otra característica biológica o del comportamiento de una persona puede ser usada para realizar la identificación, siempre que dichas características se demuestren propias y únicas de la persona a identificar. Las distintas técnicas que se están estudiando actualmente se pueden ver descritas en [A.k99], siendo:

- *Voz*: es una técnica con uno de los mayores potenciales comerciales: los servicios de atención telefónica personal, como la Banca Telefónica. Es una técnica que se lleva estudiando durante varias décadas, existiendo innumerables métodos para realizar, tanto la extracción de características, como la comparación [G.R] . Algunos métodos son dependientes del texto pronunciado (es decir, todo o parte del texto que se recita debe ser idéntico en todas las ocasiones), mientras otros son independientes del mismo (pudiéndose recitar cualquier locución para realizar la identificación). Desgraciadamente no están todavía determinados todos los factores que influyen en las locuciones, tales como la edad, las enfermedades, el comportamiento, el estado de ánimo, el canal, etc. Diversos estudios están logrando minimizar los efectos de algunos de esos factores, pero todavía queda mucho camino por andar.

Figura 2.6: Tracto Vocal.

- *Huella Dactilar*: tal y como ya se ha comentado, es, sin lugar a duda, la más estudiada y probada. Existen numerosos estudios científicos que evalúan la unicidad de la huella de una persona y, lo que es más importante, la estabilidad con el tiempo, la edad, etc. En estos aspectos es una técnica que le lleva mucha ventaja a las demás, debido a su siglo de existencia. Su captura recibe diversas formas, sobre todo últimamente, debido a la innovación tecnológica. En cuanto a la extracción de características, existen principalmente tres filosofías [LT99]: la correlación de imágenes, la extracción y comparación de minucias (uniones y terminaciones de los surcos de la huella), y la extracción y comparación de los poros del dedo.

Figura 2.7: Huella Dactilar.

- *Rostro*: es el método de identificación que nuestro cerebro usa más a menudo y de una forma más sencilla. En la actualidad existen muchos grupos de investigación trabajando en esta técnica con diversos métodos (estudios morfológicos, transformadas multiresolución, etc.). Los resultados que se están consiguiendo son bastante prometedores, aunque le falta todavía bastante hasta llegar al nivel de otras técnicas [LT99]. El gran inconveniente encontrado es la variabilidad del rostro del sujeto a lo largo del tiempo: gafas, barba, longitud del pelo, peinado, expresiones, etc.

Figura 2.8: Rostro.

- *Iris*: esta técnica fue impulsada por John G. Daugman en 1993, tal y como se muestra en [Dau93]. Los resultados obtenidos son, sin lugar a dudas, unos de los mejores de la actualidad [R.Sa],[R.Sb], teniendo en cuenta que las características en las que está basada, el patrón de la textura del iris ocular, permanece inalterable durante la vida del sujeto debido a la protección que le proporciona la córnea. Por otro lado, los estudios sobre la unicidad de sus características, la han colocado muy por encima de la huella dactilar. Su gran inconveniente es el coste de los equipos, aunque teniendo en cuenta el grado de fiabilidad alcanzado, existen numerosas aplicaciones de alta seguridad que podrían usar esta técnica.

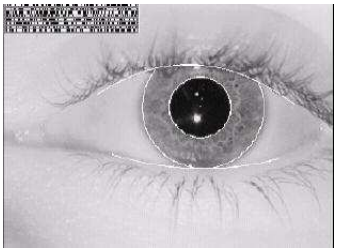


Figura 2.9: Iris.

- Oreja: desde un punto de vista forense, se ha demostrado que la oreja de un individuo posee muchas características propias del mismo. Es una técnica de estudio muy reciente y su gran inconveniente es la necesidad de que el usuario descubra su oreja frente a una cámara, lo cual puede ser incómodo en el caso

de personas con el pelo largo, o de determinados condicionantes sociales, de educación, religiosos, etc.

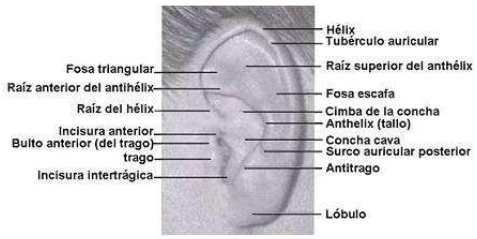


Figura 2.10: Aparato auditivo.

- *Andadura o modo particular en el que una persona camina*: Es una técnica basada en características del comportamiento, por lo que es muy susceptible de ser falseada por imitaciones. Su estudio se encuentra en la actualidad en pleno desarrollo.

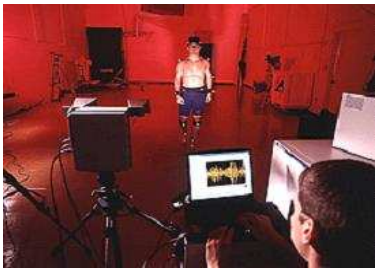


Figura 2.11: Modo particular en el que una persona camina.

- *Dinámica de teclado*: se basa en reconocer a una persona por la forma en que escribe a máquina. Se mantiene la hipótesis de que el ritmo de teclado es característico de una persona, y prototipos existentes parecen reafirmar esa hipótesis. Sin embargo, además de ser una técnica basada en el comportamiento, y por tanto potencialmente emulable, tiene la limitación de no poder ser utilizada con usuarios que no tienen facilidad a la hora de escribir a máquina.

- *ADN*: sin lugar a dudas, la única técnica capaz de identificar unívocamente a una persona. Su potencia en el campo de la identificación choca con la

dificultad en el desarrollo de sistemas automáticos de identificación en tiempo real y cómodos para el usuario. Los últimos intentos tratan de tomar la muestra mediante captación del sudor del sujeto. Sin embargo habría que estudiar la reacción de los usuarios frente a ese modo de captar la muestra.

- *Firma*: técnica en la que nos basamos, es utilizada desde antes que la huella dactilar. Esta técnica siempre ha sido cuestionada debido a la posibilidad de falsificaciones, puesto que está basada en características del comportamiento. Las nuevas tecnologías facilitan realizar, no sólo el estudio de la firma ya realizada, sino también el estudio del acto de firmar, captando mediante un bolígrafo especial o una tableta gráfica, parámetros como velocidad, paradas, posición del bolígrafo, fuerzas, etc. en el mismo acto de firmar. Existen diversos prototipos y algunos productos comerciales, pero su éxito comercial ha resultado relativamente decepcionante.

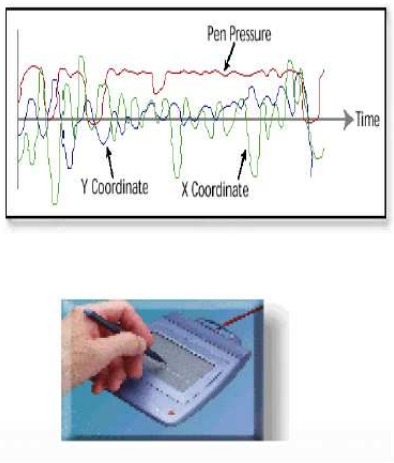


Figura 2.12: Firma.

- *Olor*: técnica muy reciente, se basa en reconocer a una persona a través de su olor corporal. Las grandes incógnitas se encuentran en ver el rendimiento de este tipo de técnica frente a perfumes, colonias, olores ambientales, contactos con otras personas, etc.

Figura 2.13: Aparato de captación del olor.

- *Exploración de la retina*: se ha demostrado que el patrón de los vasos sanguíneos de la retina presenta una mayor unicidad que el patrón del iris. Además, la casi imposible modificación de ese patrón, así como la facilidad para la detección de sujeto vivo, la hacen ser considerada la técnica más segura. Sin embargo, la forma de hacer la exploración, mediante láser, provoca un rechazo casi total por parte de los usuarios, estando sólo indicada para entornos de extrema seguridad, donde los usuarios son pocos y conscientes del grado de seguridad necesario.

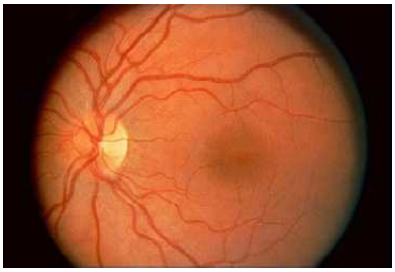


Figura 2.14: Retina.

- *Geometría del contorno de la mano y/o del dedo*: se trata de una técnica en la que se estudian diversos parámetros morfológicos de la mano (o el dedo) del usuario, tales como anchuras, alturas, etc. La técnica basada en geometría del dedo se puede considerar como una simplificación de la basada en contorno de la mano. El gran atractivo de esta técnica, debido a su simplicidad, bajo coste y mínimo tamaño del patrón, la han convertido en la técnica con mayor éxito comercial en el último par de años.

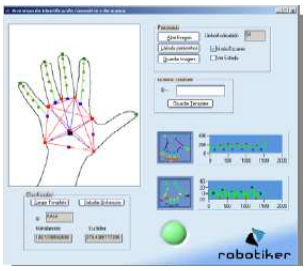


Figura 2.15: Geometría de la mano.

Todas y cada una de estas ténicas tienen sus partidarios y sus detractores. Sin embargo, lejos de lo que piensan unos y otros, se puede afirmar que no existe la técnica única, perfecta e ideal que se pueda utilizar siempre. Cada técnica tiene sus ventajas y sus inconvenientes que hace que técnicas que ofrecen unos resultados excelentes, no puedan ser usadas en muchos entornos debido al rechazo de los usuarios o, simplemente, al coste. Por otro lado, técnicas que ofrecen un nivel de seguridad inferior, por otras razones pueden ser más fácilmente empleadas en determinados entornos, al ser más importantes las ventajas que proporcionan.

2.6 Normas de evaluación

En este apartado vamos a hacer una presentación del SUBCOMITE SC37, es decir vamos a realizar una presentación del proyecto 19795, y mostraremos las diferentes partes que tiene, con una pequea introducción a cada una de ellas.
La ISO / IEC 19795-1[ISO05], fue preparada por su Comité Técnico Conjunto ISO / IEC JTC 1, Tecnología de la Información, Subcomité SC 37. De esta norma se han utilizado sólo las dos primeras partes, que versan sobre:

- ***Parte 1: Principios y marco***:

  En esta parte se establecen los principios generales para comprobar el funcionamiento de los sistemas biométricos en cuanto a tasas de error y tasas de rendimiento (número de usuarios tratados por unidad de tiempo) se refiere. Incluye la predicción del rendimiento, la comparación del mismo y cómo verificar el cumplimiento del rendimiento. Se centra únicamente en las pruebas

científicas de "rendimiento técnico" de los sistemas biométricos y los dispositivos.

Estas medidas son de aplicación general a todos los sistemas biométricos y dispositivos. Las pruebas de desempeño técnico que son específicas del dispositivo - por ejemplo, escáner de huellas digitales de calidad de imagen-, no se consideran en esta parte de la norma ISO / IEC 19795[ISO05].

- ***Parte 2: Métodos de ensayo para la evaluación tecnológica y de escenario***:

  Esta parte de la ISO / IEC 19795[ISO06] establece los requisitos y recomendaciones sobre la recopilación de datos, análisis, y la presentación de informes específicos para dos tipos principales de evaluación: evaluación de la tecnología y la evaluación de escenarios.

  La gran mayoría de las pruebas biométricas son de uno de estos dos tipos de evaluación genérica. La evaluación tecnológica, realiza evaluaciones de la inscripción y de los algoritmos de comparación por medio de muestras recogidas previamente, mientras que la evaluación de escenario evalúa sensores y algoritmos de procesamiento de las muestras obtenidas de los sujetos de prueba en tiempo real. El primero se suele usar más cuando tenemos que evaluar grandes volúmenes de muestras. El segundo se usa para la medición del rendimiento en entornos de modelado.

2.7 Planificación de la evaluación de un sistema biométrico

El hecho de evaluar un sistema para conseguir unos objetivos requiere una buena planificación. A la hora de evaluar un sistema, el experimentador deberá determinar qué sistemas se van a evaluar, aplicaciones que necesita, ver cuál es el medio que se quiere evaluar, los aspectos de rendimiento para medir, es decir, debe seguir una serie de pasos para conseguir el objetivo deseado.

Se debe obtener información sobre el sistema que vamos a evaluar con el objetivo de planificar los procedimientos de recopilación de datos. Esta información puede ser resumida con las siguientes preguntas sobre el sistema (a continuación se dan las respuesta para nuestro caso en concreto, que es la evaluación tecnológica de distintos algoritmos).

- *¿El sistema registró información en cada captura de las muestras biométricas (en nuestro caso firmas)?*

  No, pero esta información no es necesaria para la evaluación a realizar.

- *¿El sistema guardó un vector de características de cada muestra biométrica o la muestra en sí?*

  El sistema almacena las señales temporales (posición X e Y, presión, inclinación y altitud) capturadas por la tableta digitalizadora.

- *¿El sistema devuelve resultados de similitud entre la muestra y el patrón o simplemente acepta o rechaza la muestra?*

  El sistema devuelve resultados de similitud.

- *¿Está disponible el SDK (kit del software de desarrollo)?*

  El SDK es nuestro.

  Nota: este será necesario para la generalización de los patrones de alistamiento, para la extracción de características de las muestras de pruebas y para la adecuación de la generación de los resultados.

- *¿Se requieren modificaciones en el sistema para realizar la prueba?*

  No.

- *¿Las modificaciones requeridas alterarán el funcionamiento del sistema?*

  No se requieren modificaciones.

- *¿El sistema genera patrones de alistamiento independientes?*

  No, el sistema genera patrones a partir de un conjunto de muestras biométricas, por lo tanto depende de las firmas seleccionadas, dentro de las genuinas disponibles de cada usuario, para generar dicho patrón.

- *¿El sistema usa algoritmos que adaptan el patrón de usuario después de una verificación verdadera?*

  No.

- *¿Cuál es la calidad recomendada de la muestra y los umbrales de decisión para lograr nuestro objetivo?*

  La respuesta a esta pregunta es una de las motivaciones de este proyecto fin de carrera. En él se pretende dar respuesta a las resoluciones mínimas de captura para las coordenadas X e Y, así como la resolución mínima para la captura de la presión. También la frecuencia de muestreo será analizada.

- *¿Se sabe cuál es la tasa de error?*

  Las tasas de error esperadas para falsificaciones entrenadas van entre el 3 % y el 10 %, que son las típicas para algoritmos de verificación de firma manuscrita.

Las tasas de error esperadas para falsificaciones aleatorias son menores del 1 %.

Nota: esta información nos ayudará a saber si el tamaño de prueba es el adecuado.

- *¿Cuáles son los factores que influirán en el sistema?*

  Los factores que afectarán serán:

  - Factores incorporados en la estructura del experimento (resolución de la captura de coordenadas X e Y, resolución de captura de captura de presión, frecuencia de muestreo).
  - Factores controlados para formar parte de las condiciones experimentales (condiciones de laboratorio en la captura de las firmas manuscritas).
  - Factores "aleatorios".

- *¿El tamaño de la prueba depende del tamaño de la base de datos que tengamos (la cual contiene todas las muestras de firma capturadas)?*

  Sí.

Si hacemos referencia a la evaluación de escenario y a la evaluación operacional, debemos de tener en cuenta que las pruebas de funcionamiento y las posibles adaptaciones de los dispositivos al entorno de evaluación que se hagan para lograr un rendimiento óptimo, tendrán que tener lugar antes de la recolección de datos.

La base de datos que se usará para la realización de las evaluaciones, es la base de datos pública MCyT Signature (SubCorpus), contiene 100 usuarios con 25 firmas genuinas y 25 firmas falsas cada uno de ellos.

A continuación, lo idóneo es ver si con nuestra base de datos podemos hacer una prueba adecuada, es decir, comprobaremos si nuestro tamaño es el que se precisa. El tamaño de una evaluación, refiriéndonos al número de voluntarios y al número de

intentos hechos, nos permitirá medir con precisión los índices de error (ver ecuación 2.12). Cuanto más grande sea el tamaño, la prueba proporcionará unos resultados más probables.
A la hora de hacer múltiples pruebas, como el coste de la recogida de datos es tan alto se realizan evaluaciones técnicas mediante una serie de protocolos con el fin de que puedan llevarse a cabo con un esfuerzo de recopilación de datos menor.

- *Evaluación tecnológica*: es posible recoger una única BBDD fuera de línea de algoritmos que tengan patrones iguales de varios proveedores. De este modo, desvinculamos la recogida de datos y el procesamiento de señales de los subsistemas. En consecuencia, la evaluación de la tecnología fuera de línea con un corpus/base de datos normalizado nos podrá dar una buena indicación del rendimiento total del sistema.

- *Evaluación de escenario*: las evaluaciones de múltiples hipótesis pueden ser realizadas simultáneamente con una base de datos que contenga voluntarios de diferentes dispositivos. Debido a ello requerirá una mayor atención en el proceso de evaluación. El orden de presentación de los voluntarios tiene que ser aleatorios.

- *Evaluación operacional*: por lo general no permiten múltiples pruebas del mismo conjunto de datos recogidos.

2.8 Análisis de la Evaluación Biométrica

Cuando realizamos un análisis de una evaluación, debemos saber diferenciar cada uno de los parámetros a evaluar, cómo se debe hallar cada uno de los resultados que queremos obtener así como saber representar e interpretar cada uno de los resultados.
La finalidad de este proyecto es conseguir evaluar las diferentes tasas de errores para cada algoritmo a analizar y para ello debemos calcular tanto los intervalos de confianza como las varianzas.

2.8.1 False non-match rate y False reject rate

- *False non-match rate(FNMR)*: es la proporción de intentos de firmas genuinas que son declaradas falsas, al no superar el umbral de similitud con el patrón de la identidad declarada.

- *False reject rate(FRR)*: es la probabilidad de que a una persona autorizada no se le identifique, es decir, se le deniegue la firma, produciéndose un falso rechazo. Es el porcentaje de falsos rechazos entre el numero total de intentos de reconocimientos válidos.

A veces se confunden los conceptos de FNMR y FRR, no obstante se diferencian en que el FNMR no contabiliza los intentos previamente rechazados.

2.8.2 False match rate y False accept rate

- *False match rate (FMR)*: es la tasa de personas no autorizadas que son falsamente reconocidas durante una comparación de características.

- False accept rate(FAR): es la probabilidad de que una persona no autorizada sea identificada, es decir, aceptada como autorizada. Mide la frecuencia con que un usuario no autorizado, al que no debería concedérsele el acceso, se le reconoce por equivocación (se le dice que su firma es válida).

A veces se confunden los conceptos de FMR y FAR, no obstante se diferencian en que el FNMR no contabiliza los intentos previamente rechazados

2.8.3 Estimación de la varianza

La finalidad de este apartado consiste en presentar la forma en la cual se debe calcular la varianza en cada uno de los siguientes casos.

2.8.3.1 Firmas Genuinas y Firmas Falsas

El primer caso que estudiaremos será ver cómo calculamos las varianzas para el uso de firmas genuinas y firmas falsas en función del número de intentos que se hagan.

- *Si el usuario hace sólo un intento*

$$p\_estimada = \frac{1}{N} * \sum_{i=1}^{N} a_i \tag{2.1}$$

$$v\_estimada = \frac{p\_estimada * (1 - p\_estimada)}{N - 1} \tag{2.2}$$

  - N: número de usuarios
  - m: número de intentos por usuario
  - a_i: número de falsos rechazos/falsos aceptados
  - p_estimada: tasa total de falsos rechazos/falsos aceptados
  - v_estimada: varianza estimada de falsos rechazos/falsos aceptados

- *Si hacemos múltiples intentos*

$$p\_estimada = \frac{1}{m * N} * \sum_{i=1}^{N} a_i^2 \tag{2.3}$$

$$v\_estimada = \frac{1}{N - 1} * \left(\frac{1}{m_i^2 * N} * \sum_{i=1}^{N} a_i^2 - p\_estimada^2 \right) \tag{2.4}$$

  - N: número de usuarios
  - m: número de intentos por usuario
  - a_i: número de falsos rechazos/falsos aceptados
  - p_estimada: tasa total de falsos rechazos/falsos aceptados

  - v_estimada: varianza estimada de falsos rechazos/falsos aceptados

- *Si tenemos un número diferente de intentos por usuarios*

$$p\_estimada = \frac{\sum_{i=1}^{N} a_i}{\sum_{i=1}^{N} m_i} \tag{2.5}$$

$$v\_estimada = \frac{\sum_{i=1}^{N} a_i^2 - p\_estimada^2 * \sum_{i=1}^{N} a_i * m_i + p\_estimada^2 * \sum_{i=1}^{N} m_i^2}{\frac{N-1}{N} * \sum_{i=1}^{N} m_i} \tag{2.6}$$

  - N: número de usuarios
  - m: número de intentos por usuario
  - a_i: número de falsos rechazos/falsos aceptados
  - p_estimada: tasa total de falsos rechazos/aceptados
  - v_estimada: varianza estimada de falsos rechazos/aceptados

2.8.3.2 Firmas Falsas Aleatorias

Como hemos dicho en la raíz de este apartado, el modo de calcular la varianza difiere dependiendo de las firmas que usemos. En este caso al usar las firmas falsas aleatorias el cálculo es el siguiente:

$$q\_estimada = \frac{1}{m * n * (N-1)} * \sum_{i=1}^{N} \sum_{j=1}^{N} b_{ij} \tag{2.7}$$

$$v\_estimada = \frac{1}{m^2 * N^2 * (N-1)^2} * \sum_{i=1}^{N} \left(c_i^2 - d_i^2\right) - \frac{4}{N} * q\_estimada \tag{2.8}$$

- N: número de usuarios
- m: número de firmas falsas aleatorias por usuario
- b_{ij}: número de firmas del usuario i que han sido aceptados por el usuario j

- c_i: número de firmas falsas aleatorias de otros usuarios que han sido aceptados como del usuario i
- d_i: número de firmas falsas aleatorias del usuario i que han sido aceptados como de otros usuarios
- q_estimada: tasa total de falsos aceptados
- v_estimada: varianza estimada de falsos aceptados

2.8.4 Intervalos de Confianza

Con un número elevado de intentos y aplicando el teorema del límite central veremos la tasa de error sigue una distribución aproximadamente normal. Debido a ello, un intervalo de confianza para el verdadero valor de la tasa de error p es:

$$p\_estimada \pm z_{1-\frac{\alpha}{2}} * \sqrt{v_e stimada} \tag{2.9}$$

siendo v_estimada cuanquiera de las calculadas anteriormente.

El valor que tome z depende del nivel de confianza:

- Si tenemos un nivel de confianza del 90 % tendrá un valor de 1.64.
- Si tenemos un nivel de confianza del 95 % tendrá un valor de 1.96.

Por ejemplo: ¿Cuál deber ser el tamaño de la base de datos para estimar la porporción de firmas falsas con un nivel de confianza del 90 % y una tasa de error inferior al 30 % si una base de datos de 5000 posee 2500 falsas?

Partimos de la ecuación 2.9 y suponenos que nuestra varianza estimada es la mencionada en la ecuación 3.2. Por tanto el tamaño de la base de datos será:

$$N \geq \frac{z_{1-\frac{\alpha}{2}} * p\_estimada * (1 - p\_estimada)}{E^2} + 1 \tag{2.10}$$

Siendo E aquello que sumamos y restamos a p_estimada, es decir, el error.

Luego sustituyendo por los datos que nos proporcionan en el enunciado, tendremos un tamaño:

$$p\_estimada = \frac{nmerodefallos}{nmerototaldedatos} = \frac{2500}{5000} = 0{,}5 \tag{2.11}$$

$$N \geq \frac{1{,}64^2 * 0{,}5 * (1 - 0{,}5)}{0{,}3^2} + 1 = 8{,}5 \approx 9 \tag{2.12}$$

Si nos centramos en el intervalo de confianza, para este caso tendríamos:
0.5 ± 0.3 (si hacemos la operación inversa, sabiendo que el tamaño de la muestra es 9, se puede comprobar que da esta tasa de error.)

2.8.5 Representación Gráfica

Para finalizar una evaluación, deberemos hallar el rendimiento del sistema. El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y el fallo de tasa de alistamiento (Failure-to-enroll Rate, FTR o FER). En los sistemas biométricos reales el FAR y el FRR pueden transformarse en los demás cambiando cierto parámetro.

2.8.5.1 Curva FRR-FAR

Es la curva que nos permite representar los falsos rechazos y los falsos aceptados (tanto para firmas falsas entrenadas como para firmas falsas aleatorias). A partir de ella podemos ver el rendimiento del sistema. Para ello, es necesario hallar la tasa de cruce.

2.8.5.2 Curva ROC

También denominada como curva característica de funcionamiento del receptor o Receiver Operating Curve. Es un gráfico que muestra cómo varía la FRR en función de FAR de acuerdo a un umbral de decisión. Es una función dibujada sobre los ejes de coordenadas cartesianos cuyo eje de ordenadas es FRR o FNMR y cuyo eje de abscisas es FAR o FMR.

2.8.5.3 Curva DET

Curva también denominada Detection Error Trade-off. Nos permite representar lo mismo que la curva ROC, sin embargo se diferencia en que la cueva DET se representa con los ejes en base logarítmica.

2.8.6 Información Adicional: Detalles en los Informes de una Prueba

El rendimiento de un sistema biométrico y de una evaluación biométrica, analizado mediante la curva DET, los índices de error... depende del tipo de prueba, la aplicación y la población usada.

Para que estas medidas tengan una correcta interpretación se deberá facilitar la siguiente información:

- Detalles del sistema(s) de la prueba. Esto debería incluir a parte del componente biométrico, los factores tales como la interfaz de usuario... que también influyen en el rendimiento.
- El tipo de evaluación:
  - Evaluación de la tecnología: se deberá facilitar los detalles del corpus utilizado.
  - Evaluación de escenarios: se cumplimentará con los detalles del escenario de prueba.

  - Evaluación operacional: se facilitarán los detalles de la aplicación operativa.

- El tamaño de evaluación:
  - Número de usuarios.
  - Número de dedos, manos, ojos ... inscritos por cada usuario que serán evaluados.
  - Número de intentos efectuados por cada usuario en la prueba.
  - Número de transacciones por sujeto de prueba en cada intento.
- Datos demográficos de la población de prueba (edad, sexo...).
- Datos sobre el entorno de prueba.
- La separación de tiempo entre la matrícula y las transacciones de prueba.
- La calidad y los umbrales de decisión utilizados durante la recolección de datos.
- Información detallada sobre cómo los factores que podrían afectar al rendimiento fueron controlados (véase el anexo C de la norma 19795 [ISO05]).
- Información detallada sobre el procedimiento seguido en la prueba, por ejemplo, políticas para determinar los fallos de inscripción.
- Información detallada sobre el nivel de formación, la familiarización, y la habituación de la población de prueba en el uso del sistema.
- Detalles de los casos anormales y los datos excluidos del análisis.
- La incertidumbre estimada (y el método de estimación).
- Las desviaciones de las directrices de esta parte de la norma ISO / IEC 19795 también deben ser explicadas.

Capítulo 3

Introducción Firma Manuscrita

En este capítulo nos centraremos en lo que es en sí nuestro objeto de evaluación, es decir, conoceremos a fondo el significado de una firma, su origen, los componentes que posee as como el procedimiento a seguir para su reconocimiento a la hora de hacer una evaluación Por otro lado expondremos los parámetros a estudiar junto con los algoritmos que nos ayudarán en el estudio.

3.1 Firma Manuscrita

Según la Real Academia Española, la primera acepción que tuvo la firma fue Nombre y Apellido o título, de una persona la cual pone al pie de un documento escrito de mano propia o ajena, para darle autenticidad o para verse obligado a hacer lo que el documento estipula.

Para nosotros, y a lo que nos referiremos a lo largo de nuestro proyecto, una firma será referida al proceso de creación de una rúbrica por parte de un individuo, en el que se ha sustituido la pluma original por una pluma de una tableta digitalizada.

3.2 Orígenes de la firma manuscrita

No existe en nuestro Derecho, una teoría sobre la firma, sus elementos, consecuencias o su concepto y las pocas referencias que existen son obras de Derecho Notarial.

En Roma, existía la Manufirmatio, que consistía en una ceremonia en que leído el documento por su autor, o el funcionario, se colocaba desenrollado y extendido sobre la mesa del escribano y luego se pasaba la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo. Se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que un requisito, la Manufirmatio era en sí misma parte del espectáculo solemne en que se realizaba el acto. En la Edad Media, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que la mayoría de los ciudadanos no sabían ni leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos.

La diferenciación entre firmas y signos hizo que se empezase a entender que aquellas eran, más que simples signos, la inscripción manuscrita del nombre o de los apellidos. Generalmente los particulares la estampaban en los documentos de las transacciones comerciales, haciendo así que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.

3.3 Características de la firma manuscrita

La caracterstica más importante de un alfabeto debe ser que las diferencias entre distintos caracteres son mayores que las diferencias entre distintas muestras del mismo carácter incluso escritas por diversos autores. Pero hay casos en nuestro alfabeto en que esto no es del todo cierto y por ejemplo las letra I (i mayúscula) y la l (L minúscula) las diferenciamos más por el contexto en el que se encuentran que por su apariencia.

Podemos caracterizar una firma si consta de los siguientes rasgos:

- *Identificativa*: Sirve para autentificar quién es el autor del documento.
- *Declarativa*: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.
- *Probatoria*: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma.

En el caso de las firmas, en muchas ocasiones ni nosotros mismos somos capaces de reconocer caracteres en ellas, simplemente vemos trazos, formas que nos dan información, pero no es una información clara ni exacta. De manera que, incluso dos firmas del mismo autor(figura 3.1) pueden diferir en muchos detalles(figura 3.1).

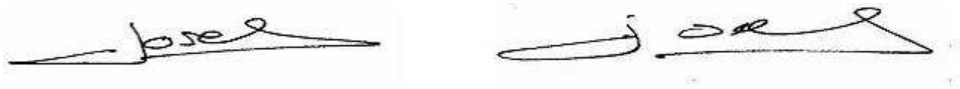


Figura 1. Firma patrón Figura 2. Variación de la firma

Figura 3.1: Firma patrón (original) y variación de la firma original.

Por tanto, parece obvio que uno de los objetivos sea fijarse y centrarse en las formas más características y relevantes de la firma e intentar obviar los detalles menos significativos, o por lo menos no darles demasiada importancia.

3.4 Elementos de la firma manuscrita

Es necesario distinguir entre:

- *Elementos formales*: Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la misma:
  - *Firma como signo personal*: La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta

característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

- *Animas signandi*. Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento.

- *Elementos funcionales*: Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función, identificadora y autentificadora. La firma, al ser un elemento personal, se ha utilizado y se utiliza para plasmar la identidad del autor. Por ello la falsificación de la firma es uno de los métodos más habituales para suplantar a una persona, generalmente con un fin económico. La falsificación de firmas se puede clasificar en dos clases:

  - *Las falsificaciones burdas*: son las más frecuentes y son aquellas en las que el falsificador desconoce la firma original y por tanto las similitudes son pocas o casuales.

  - *Las falsificaciones expertas*: son poco frecuentes y están realizadas por un falsificador con entrenamiento, el cual conoce la firma y la reproduce con cierta maestría.

3.5 Reconocimiento de la firma manuscrita

Se llevará un proceso de reconocimiento de firmas para evitar dichas falsificaciones el cual se ilustra en la figura 3.2.

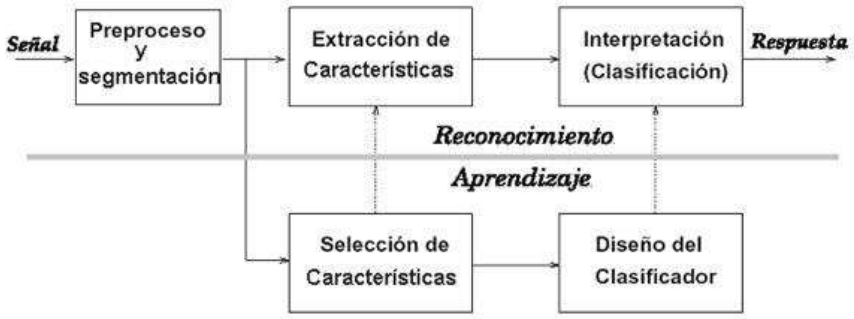


Figura 3.2: Sistema de Reconocimiento.

El reconocimiento de firmas se puede realizar por dos métodos:

- *Métodos estáticos*: Son aquellos métodos que nos permiten verificar características estáticas biométricas que no varían con el tiempo. Suelen ser llamados también off-line, debido a que tanto la inscripción como las pruebas se realizan con muestras previamente. Todos ellos se basan en el reconocimiento de patrones. Suelen ser empleados para la verificación de:
  - Huellas dactilares.
  - Biometría del ojo: por un lado, el iris y por otro, la retina.
  - Geometría de la mano.
  - ADN.
  - Emisiones térmicas.
  - Características estáticas de la cara.
  - Venas de muñecas y manos.
  - Composición química del olor corporal.
  - Rayas de la mano (quiromancia).
  - Poros de la piel.
- Métodos dinámicos: Son aquellos métodos que nos permiten verificar características dinámicas biométricas que pueden variar con el tiempo. Suelen ser

llamados también on-line, debido a que la inscripción o clasificación de las muestras se realiza en el momento en que es capturada la(s) misma(s). No es preciso almacenar los datos, aunque se aconseja hacerlo ya que esto permite procesarlos posteriormente, en caso de ser necesario. Suelen ser empleados para la verificación de:

- Gestos y movimiento corporal.
- Dinámica del tecleo.
- Manuscritos.
- Firma (nuestro caso).
- Voz.

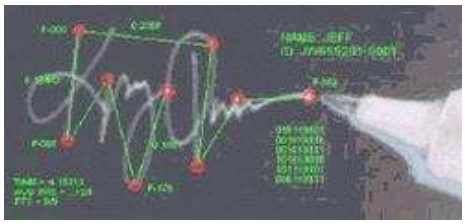


Figura 3.3: Método Dinámico.

3.6 Dispositivos de captura de firma

Las herramientas biométricas, generalmente lectores, permiten un control de acceso sin necesidad de personal que verifique las identificaciones. También, es útil para el control de acceso de grandes volúmenes de personas.

En nuestro caso, las herramientas que usaremos serán las tabletas gráficas o digitaligitalizadora. Dicha tabletas, son dispositivos que permiten al usuario introducir gráficos o dibujos a mano, tal como lo haría con lápiz y papel. También permite apuntar y señalar los objetos que se encuentran en la pantalla. Consiste en una superficie plana sobre la que el usuario puede dibujar una imagen utilizando la lapicera que viene junto a la tableta. En algunas tabletas la imagen no aparece en la tableta sino que se muestra en la pantalla de la computadora, en otras como los últimos modelos de las mejores marcas se puede ver la pantalla en la tableta. Algunas tabletas digitalizadoras están diseñadas para ser utilizadas reemplazando al ratón como el dispositivo apuntador principal. Por último aclararemos que hay dos tipos de tabletas:

- *Pasivas*: hacen uso de inducción electromagnética, donde la malla de alambres horizontal y vertical de la tableta operan tanto transmitiendo la señal como recibiéndola. La tableta digitalizadora genera una señal electromagnética, que es recibida por el circuito resonante que se encuentra en el lápiz. Cuando la tableta cambia a modo de recepción, lee la señal generada por el lapicero; esta información, además de las coordenadas en que se encuentra puede incluir información sobre la presión, botones en el lápiz o el ángulo en algunas tabletas.

- *Activas*: llevan pilas en el interior de la lapicera, que genera y transmite la señal a la tableta. Por eso son más grandes y pesan más que las tabletas pasivas. Por otra parte, eliminando la necesidad de alimentar al lápiz, la tableta puede escuchar la señal del lápiz constantemente, sin tener que alternar entre modo de recepción y transmisión constantemente.

Algunos ejemplos de estas son:(ver figura 3.4)

Figura 3.4: Tabletas gráficas.

3.7 Parámetros en estudio

En este apartado explicaremos en qué son y en qué consiste cada uno de los parámetros que vamos a evaluar.

3.7.1 Presión

En la identificación de una persona, a través de su escritura / firma manuscrita, la presión es uno de los elementos estructurales de grafismo que siempre está presente, y que resulta esencial para tales fines. Conforme a la doctrina en la materia, para unos, la presión es de fácil observación, para otros, no lo es tanto, y demanda mucha observación y ponderación en su estudio y análisis.

La presión se puede definir como la fuerza o energía con la que se asienta sobre el receptor, en nuestro caso la tableta gráfica, para producir o ejecutarla escritura y/o firma manuscrita. Esta, no es constante en una escritura y/o firma manuscrita, esta íntimamente ligada a los movimientos de extensión, rotación y flexión de la parte del órgano humano utilizado para escribir.

En la escritura o firma manuscrita, habrá unas secciones con más presión escritural que otras; es como un circuito de una pista de carreras, habrá zonas o sectores donde un vehículo correrá más rápido, y otros sectores donde disminuirá la velocidad y en consecuencia tendrá más agarre en el piso. Por consiguiente podremos decir, que a menor velocidad, más presión y a mayor velocidad, menor presión.

Generalmente en las tabletas gráficas avanzadas, el rango de la presión varían de 1024 a 2048. En nuestro caso, la tableta que usamos capta una presión de 1024 y lo que vamos a intentar es ver hasta qué punto podemos reducir esta resolución, escalándola, sin perder calidad en la imagen de la firma.

A grandes rasgos, puesto que en el capítulo 4 se explicará más detallado cómo se realiza el escalado, lo que haremos es escalar el rango de precisión que tenemos dividiendo el mismo por un factor de escalar que va a tomar valores de 0 a 6. El valor 0 lo tomará cuando no queramos escalar el parámetro. Por lo que las resoluciones,

como rango de presión posible, a estudiar serán las siguientes: 1024. 512, 256, 128, 64, 32 y 16.

3.7.2 Posición (ejes X e Y)

Con la posición nos referimos a las dimensiones que pueden llegar a tener las tabletas gráficas. Normalmente, si son tabletas avanzadas, suelen tener un valor de 2000 a 5000 puntos por pulgadas (PPP).

En nuestro caso, usamos una tableta que posee 2500 puntos por pulgadas (PPP).

Para la posición, los niveles de escalados serán los mismos que para la presión. Escalaremos tomando valores de 0 a 6, siendo el valor 0 usado para cuando no queremos escalar este parámetro. Por lo que las resoluciones a estudiar, definidas en puntos por pulgada, serán las siguientes: 2500, 1250, 625, 312, 156, 78, 39.

3.7.3 Frecuencia de muestreo

La frecuencia de muestreo se puede definir como el número de muestras por unidad de tiempo que se toman de una señal continua para producir una señal discreta, durante el proceso necesario para convertirla de analógica en digital. Como todas las frecuencias, generalmente se expresa en hercios (Hz, ciclos por segundo) o múltiplos suyos, como el kilohercio (kHz), aunque pueden utilizarse otras magnitudes.

En las tabletas gráficas avanzadas, normalmente suelen tener un valor de 100 a 200Hz. En nuestro caso, la tableta que usamos es de 100 Hz, y lo que buscamos es intentar escalar dicho valor hasta el punto en el que empecemos a perder calidad en la imagen de la firma.

En este caso, los niveles de sub-muestreo estudiados son menores que en el caso anterior. Escalaremos tomando un factor de escala de 0 a 4. Por lo que las frecuencias de muestreo, en Hz, que estudiaremos serán: 100, 50, 25, 12,5, 6.25

3.8 Introducción a los algoritmos de estudio

Para evaluar nuestro sistema usaremos tres algoritmos desarrollados en el grupo de investigación GUTI, GMM, DTW y la combinación de ambos. A continuación nos centraremos en explicar cada uno de ellos de manera detallada.

3.8.1 Algoritmo de Modelo de Mezclas Gaussianas/Gaussians Mixture Modelling (GMM)

Gaussians Mixture Modelling (GMM) [And03],[O. 07b], es una técnica muy conocida y muy usada y referenciada para el reconocimiento de patrones. La teoría GMM se conocía desde hace mucho tiempo, pero no fue hasta que se desarrollaron los algoritmos de maximización [Bil98], una técnica útil para el reconocimiento de patrones. Una de las aplicaciones más conocidas a la biometría proviene de Reynolds [RQD00]. GMM ha sido utilizado con éxito en las técnicas de la biometría como el reconocimiento de voz [RQD00], geometría de la mano [SRSAGM00] y la verificación de la firma [And03].

GMM se basa en la representación de las características biométricas como una combinación lineal ponderada de las distribuciones de Gauss (véase ecuación 3.1), GMM tiene la capacidad de obtener modelos de buen funcionamiento de la distribución probabilística del conjunto de las funciones utilizadas para reconocimiento de patrones. La función de probabilidad se define como la suma ponderada de funciones de densidad de probabilidad de Gauss, a saber:

$$p\left(\vec{x}\ /\lambda\right) = \sum_{i=1}^{M} c_i * b_i\left(\vec{x}\right) \tag{3.1}$$

donde M es el número de elementos genéticamente y son los coeficientes de ponderación aplicable a cada función de probabilidad de Gauss, que se han de cumplir para que p sea una función de densidad adecuada. Se debe saber que:

$$\sum_{i=1}^{M} c_i = 1 \tag{3.2}$$

Las densidades gausianas tiene la siguiente forma:

$$b_i\left(\vec{x}\right) = \frac{1}{\left(2\pi^{\frac{L}{2}}\right) * \| \sum \|^{\frac{1}{2}}} * e^{\frac{1}{2} * \left(\vec{x} - \vec{y_i}\right)^T * \sum_i^{-1} \left(\vec{x} - \vec{y_i}\right)} \tag{3.3}$$

donde μ_l y $\sum_i$, son el vector de media y la matriz de covarianza, respectivamente, definidos para cada densidad de Gauss, y $\vec{x}$ es el vector de características que representa la firma manuscrita.

Los tres elementos que definen a cada modelo de GMM: el vector de medias, matriz

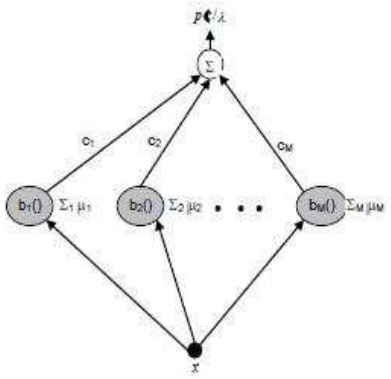


Figura 3.5: Representación del modelo de mezcla de gaussianas.

de covarianza y el coeficiente de ponderación, se agrupan en un vector landa que representan a cada usuario:

$$\lambda_l = \left\{ \vec{\mu_l}, \sum_i, c_i \right\} \tag{3.4}$$

Donde s es el número de usuarios del sistema.

3.8.2 Dynaminc Time Warping (DTW)

Dynaminc Time Warping (DTW), [SC78], es una técnica bastante conocida y muy referenciada para la verificación de firmas on-line. Tiene su origen en el campo de reconocimiento de voz [SC78].

Uno de los primeros intentos de utilizar con éxito dicho algoritmo para la verificación manuscrita proviene de Sato y Kogure [Y. 82].

DTW consiste en la alineación del eje temporal entre el patrón, p, y la(s) muestra(s). Una vez que tengamos la distancia entre dos puntos (patrón y muetsra), la medida se realiza de manera iterativa.

El alineamiento se puede hacer tanto en la forma de onda de las características extraídas de la firma, es decir, si éstas se han adquirido online, o bien en la misma imagen de la firma si la adquisición de la misma fue offline. Las firmas de una misma persona suelen ser bastantes parecidas entre sí, por lo que se necesitará poca distorsión para alinearse con el modelo de referencia, mientras que las firmas de otros usuarios o falsificadores necesitarn bastante distorsión.

En primer lugar, construye una matriz de distancia entre el patrón y los puntos de muestreo y a continuación encuentra la mejor manera de alinear la muestra con el patrón, (ver figura 3.6).

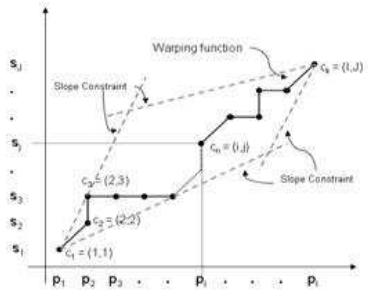


Figura 3.6: Alineamiento del patrón y la muestra.

Existen algunas restricciones para la matriz de distancias para intentar reducir al mínimo el número de puntos a calcular.

3.8.3 DTW+GMM

El algoritmo DTW+GMM, [O. 07a], consiste en una combinación de los dos algoritmos descritos anteriormente, DTW y GMM. El proceso que se lleva a cabo es el siguiente (ver figura 3.7):

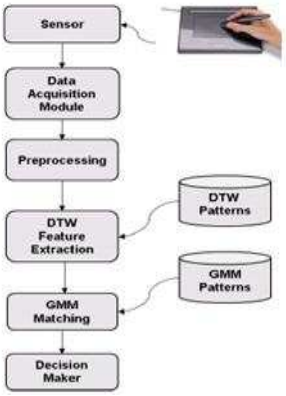


Figura 3.7: Esquema del sistema de identificación automática.

EL algoritmo DTW se utilizará para eliminar la variabilidad intrínseca de la firma del usuario mediante la armonización de las señales adquiridas de tabletas digitales con los modelos del usuario. Con ello obtenemos unas características denominadas pseudo-distancias. Por otro lado, el GMM se usará para el modelado de la distribución probabilística de la serie de pseudo-distancias y permitirá calcular el cociente de probabilidad entre las firmas del usuario y su modelo almacenado.

La firma manuscrita pertenece a la biometría de comportamiento, de modo que las muestras de la firma de un mismo individuo pueden variar intrínsecamente en cuanto a forma y tiempo se refiere. DTW se utiliza como un alineamiento de tiempo no lineal tratando de minimizar el impacto de estas variaciones. Por otra parte, GMM es ampliamente utilizado como la modelización estadística paramétrica en muchas aplicaciones de reconocimiento de patrones. En GMM, las distribuciones de probabilidad continuas son modeladas por una mezcla ponderada de las densidades para ser utilizadas para evaluar la probabilidad de la muestra de ser auténtica o falsa.

Capítulo 4

Diseño, Arquitectura y Desarrollo

En este capítulo nos centraremos en describir cómo se ha diseñado, qué forma tiene y cómo funciona nuestro proyecto.

4.1 Introducción

Uno de los principales problemas que se pueden encontrar en el desarrollo, prueba y evaluación de prestaciones sistemas biométricos de reconocimiento, tanto en la identificación como en la verificación, es la falta de grandes bases de datos multimodales públicas adquiridas en condiciones reales de trabajo. Las bases de datos públicas existentes son: el PP NIST 4 grupos de imágenes de huellas dactilares [O.], FVC200x [Y. 82] bases de datos de huellas dactilares, y el de Investigación de Philips Base de datos de Laboratorios Firma [RQD00].

En este contexto, el Laboratorio de Investigación de Biométrica - ATV, de la Universidad Politécnica de Madrid, desarrolló el proyecto MCYT, en el cual nosotros nos basaremos para llevar a cabo nuestra evaluación.

Para la creación de la base de datos MCYT se ha tenido muy en cuenta,(i) el número de individuos inscritos, (ii) el número de modalidades por individuo y (iii) el número de muestras para cada modalidad (que debe incluir los diversos factores

que se pueden encontrar en el proceso de adquisición). El diseño de una base de datos multimodal busca la maximización de la cada uno de ellos, es decir, tener a tantas personas como sea posible, así como número posible de modalidades y / o de muestras.

La captura de las firmas manuscritas se realizó de manera dinámica, mediante una tableta digitalizada (Wacom Intous 2). Este dispositivo permite firmar igual que con un bolígrafo convencional.

La resolución que posee esta tableta es de 2540 líneas por pulgadas (100líneas/mm), y la precisión es de $\pm$ 0.25 mm. La altura máxima de detección es de 10 mm y el área de captura es de 127x97 mm.

Para realizar la captura, esta tableta capturó las siguientes secuencias en tiempo discreto (entre corchetes su resolución):

- Posición en el eje x, x_t: [0-12 700], lo que corresponde de 0-127 mm.
- Posición en el eje y, y_t: [0-9700] correspondiente a 0-97 mm.
- Presión ejercida por la pluma, p_t: [0-1024].
- Ángulo de azimut de la pluma con respecto a la pastilla, g_t: [0-3600], lo que corresponde a 0º - 360º.
- Ángulo de altitud de la pluma con el respeto al comprimido: [300-900], que corresponde a 30º - 90º.

La frecuencia de muestreo de las señales adquiridas se estableció en 100 Hz.

Para elaborar nuestro trabajo, partimos de esta base de datos, MCyT, en su modalidad de firma manuscrita. La base de datos cuenta con 100 usuarios. Cada usuario n, posee 25 muestras de su propia firma (en grupos de 5 muestras) y 25 falsificaciones (5 muestras de cada usuario, desde el usuario n-1 hasta el usuario n-5).

Las falsificaciones almacenadas en la base de datos, son de tipo entradas ya que cada impostor repite varias veces las firmas de la víctima hasta considerar su

imitación lo suficientemente buena antes de que dicha falsificación sea adquirida y almacenada definitivamente.

4.2 Primera Parte:Evaluación del impacto de la resolución en la captura de la señales X,Y,P y la frecuencia de muestreo en el rendimiento de los algoritmos de firma manuscrita.

EL objetivo de la primera parte consiste en evaluar cuál es el impacto que tiene la resolución de captura en las señales X e Y, en la presión, así como el impacto de la frecuencia de muestreo en el rendimiento de los algoritmos de verificación de firma manuscrita.

4.2.1 Lectura de la base de datos

Comenzamos leyendo la base de datos. Para ello, nos ayudamos de una función facilitada por los creadores de la base de datos MCyT, "leer_firma.m", a la que le pasamos la ruta donde tenemos almacenada la base de datos, el número de usuario, el número de la firma y si es genuina o falsa la misma (1 en caso de ser genuina y 0 en caso de ser falsa). De este modo, obtenemos toda la información necesaria que caracteriza una firma:

datos= [x,y,t,button,az,in,p],num_usuario, num_firma, gen.

4.2.1.1 Modificación de las resoluciones para las señales X,Y,P y Frecuencia de muestreo

El segundo paso es escalar la firma para adaptar su resolución a la deseada. En el escalado nos centraremos solo en 4 parámetros:

- x,y,(dimensiones de la tableta donde firma el usuario).
- p(presión).
- t (frecuencia).

Para su realización necesitaremos un factor de escala, el cual será almacenado en un vector. Dicho vector contendrá los factores de escala pertenecientes a los cuatro parámetros mencionados anteriormente y tomarán valores desde 0 a 6 en el caso de que escalemos los tres primeros parámetros y de 0 a 4 cuando escalemos la frecuencia. Usaremos el valor 0 cuando no queramos escalar ninguno de ellos. De este modo, al escalar, los niveles de resolución que obtendremos son:

Factor escala 0	Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	Parámetro
12699	6349	3174	1587	793	396	198	X
9649	4824	2412	1206	603	301	150	Y
1024	512	256	128	64	32	16	P
100	50	25	12.5	6.25	-	-	T

Tabla 4.1: Niveles de resolución en función del factor de escala.

Dichos valores son seleccionados para evaluar cómo afectan en el rendimiento de diferentes algoritmos de verificación de firma manuscrita. La función que nos permite hacer el escalado es “escalado.m”. Esta función se encarga de escalar los 4 parámetros. Para ello necesita saber el factor de escala y la firma a escalar.

4.2.2 Cálculo de patrones

Para poder obtener similitudes entre las firmas, lo primero es crear el modelo del usuario con el cual las compararemos. Para ello, calculamos unos patrones que nos ayudarán a ver cuanto se parecen las firmas entre sí.

Cada usuario consta de un único patrón calculado a través de 10 firmas genuinas de la base de datos MCyT. Este patrón por tanto, nos definirá cómo es la firma original del usuario.

La función que nos ayuda a obtener los patrones es:

“calcularPatrones.m”.

4.2.3 Cálculo de Similitudes

El objetivo del cálculo de las similitudes, es comprobar la semejanza de las firmas con el patrón de la identidad declarada.

Para conseguir dicho fin, se enfrentaran cada una de las firmas de cada usuario (firmas genuinas, firmas falsas entrenadas y firmas falsas aleatorias) al patrón. Como firmas aleatorias, se tomarán firmas originales de otros usuarios.

La función que nos permite obtener la matriz de similitudes de las firmas manuscritas es:

"calcularSimilitudes.m".

4.2.4 Simulaciones

Una vez escalada la firma realizamos los dos pasos anteriores [ver apartado 4.2.3 y 4.2.4] N veces (en nuestro caso en particular se realizarán 100 veces).

El hecho de realizar N veces las simulaciones es debido a que pretendemos obtener unas tasas de error más precisas, que no dependan tanto de las firmas usadas como muestras para la creación del patrón y el cálculo de similitudes. En definitiva, lo que buscamos es tener una mayor información así como una mayor base estadística para poder calcular las tasas de error...

El proceso del cálculo de patrones como el cálculo de similitudes se realizarán para todos los algoritmos (GMM, DTW, DTW+GMM) tanto escalando firmas como sin escalar las mismas y para cada uno de los escalados.

Figura 4.1: Proceso de obtención de similitudes.

4.2.5 Ánalisis de Resultados

Para el análisis propiamente dicho se va a proceder del siguiente modo:

- Haremos un análisis general, en él calcularemos la tasa de error existente por cada usuario (falsos rechazos, falsos aceptados tanto para firmas falsas entrenadas como firmas falsas aleatorias) y en función de unos umbrales. Por último representaremos las curvas FRR-FAR (falsos rechazos-falsos aceptados), ROC y DET (igual que la ROC pero en base logarítmica).

- A partir de los datos anteriores, se calcularan el valor "Equal Error Rate" (EER), tanto para firmas falsas entrenadas, como para firmas falsas aleatorias. A partir de estos valores, se realizará un análisis de la distribución de los errores por usuario.

En el primer análisis, normalizaremos la matriz de las similitudes. Sabemos que tenemos una matriz por usuario y en función de si son firmas genuinas, falsas aleatorias

y firmas falsas entrenadas. Normalizamos con el fin de que todas las matrices de similitudes tengan el mismo rango de valores y que estos siempre vayan de 0 a 100 para poder realizar comparaciones entre distintos algoritmos. Con los scores normalizamos, damos paso a obtener tanto los falsos rechazos (decir que una firma es falsa cuando es verdadera), los falsos de las firmas falsas entrenadas aceptados (decir que una firma es verdadera cuando es falsa) como los falsos aceptados de las firmas falsas aleatorias. Estos se calculan comparando cada una de la matriz de similitudes, scores, con cada uno de los umbrales que definimos (se definen cien umbrales entre el valor 0 y el 100).

La función que nos permite hallar las tasas de error es "resultados.m", la cual necesita para el cálculo la matriz de similitudes.

A partir de ellos, obtenemos la tasa de error de cruce entre el ratio de falso rechazo y el ratio de falsa aceptación, o "Equal Error Rate"(EER). Es el valor en el que la tasa de falsos aceptados y falsos rechazos es el mismo. Este cálculo se hará tanto con las firmas falsas entrenadas como con las firmas falsas aleatorias.

Este valor se obtendrá con la función "calcularEER".Dicha función a parte de calcularnos la tasa de cruce también nos calculará el umbral que usaremos posteriormente para hallar el error medio por usuario.

Por último, representaremos cada una de las curvas:

- **Curvas FRR-FAR**: en ella representamos los falsos rechazos y los falsos aceptados (tanto para firmas falsas entrenadas como para firmas falsas entrenadas) hallados previamente en la fase de obtención de resultados en función del umbral utilizado. La función que nos permite hacer la representación gráfica de esta curva es "representarGraficaFrrFar.m".

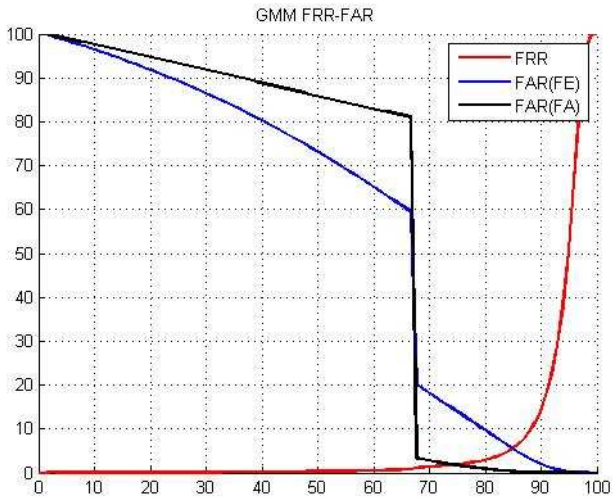


Figura 4.2: Curva FRR-FAR.

- **Curva ROC**: gráfica en la que representamos los falsos rechazos frente a las falsas aceptaciones.

  La función que nos permite hacer la representación gráfica de esta curva es "representarGraficaRoc.m".

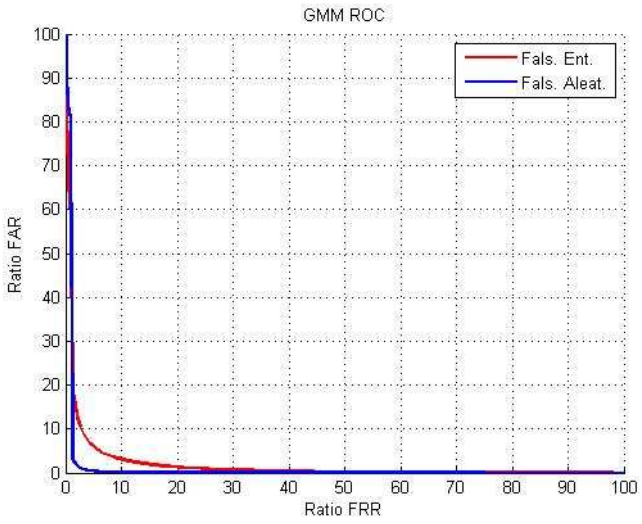


Figura 4.3: Curva ROC.

- **Curva DET**: gráfica igual que la anterior citada pero con las tasas de error en escala logarítmica.

  La función que nos permite hacer la representación gráfica de esta curva es "representarGraficaDet.m".

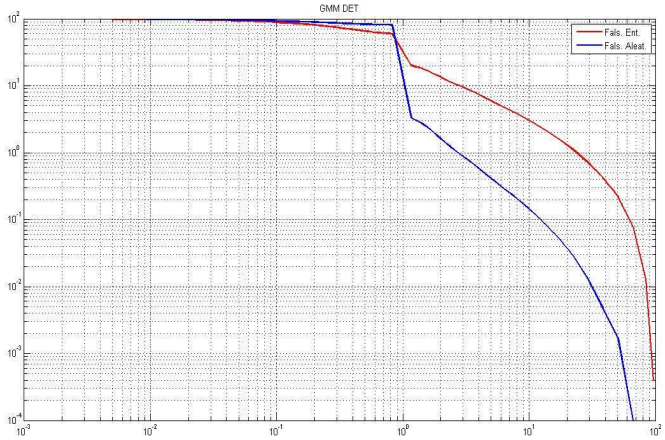


Figura 4.4: Curva DET.

A continuación en la figura 4.5, presentamos un esquema donde se pueden ver los pasos que se han seguido para la obtención de los resultados.

Figura 4.5: Proceso para el análisis de los resultados.

4.3 Segunda parte:: Estudio del impacto en el rendimiento de los algoritmos de la cantidad de información, la complejidad y la estabilidad de las firmas de los usuarios.

Figura 4.6: Esquema del proceso seguido.

El objetivo de esta segunda parte es analizar diferentes aspectos de la firma, como el acto de firmar, que nos pueda indicar si la firma de un usuario es más o menos segura ... El anexo B de la norma ISO/IEC 19794-11 [ISO09] define 3 aspectos y su forma de medirlos, para ver cuanto de segura puede ser la firma de un usuario. Estos son los siguientes:

4.3.1 Cantidad de información / Cantidad de puntos

Este aspecto de la cantidad podría estar relacionado con la resolución de la tableta digitalizadora, pero es más importante relacionarlo con la rapidez con que escribe la persona su firma. Si se firma demasiado rápido, se registran coordenadas insuficientes y como resultado tenemos escasez de datos para analizar. Este caso puede relacionarse con gente que usa como firma sus iniciales y lo hace de manera muy rápida. Normalmente, sus iniciales pueden tener la suficiente complejidad y ser muy coherente pero suelen ser rechazadas en el proceso de inscripción.

La cantidad de datos es fácil de medir mediante el conteo del número de puntos digitalizados (grabados) y garantizando que su total está por encima de un mínimo aceptable.

Mediante la función "ObtencionPuntos.m", como su propio nombre indica, obtenemos el número de puntos de las firmas de cada usuario y hacemos un promediado para saber aproximadamente con cuantos puntos de media firma cada usuario. Representamos gráficamente la media por usuario. A través de estos datos, dividimos nuestra base de datos en tres partes, cada parte representará un tipo de usuarios:

- Aquellos con firmas muy cortas (por debajo del percentil 25)
- Aquellos con firmas de longitud alrededor de la media (entre el percentil 25 y el 75)
- Aquellos con firmas muy largas (por encima del percentil 75)

Una vez realizada la división, realizaremos una evaluación del rendimiento de los algoritmos para cada una de estas sub-bases de datos, es decir, realizaremos todos

los pasos seguidos en la primera y segunda parte para observar qué ocurre cuando unas firmas poseen mayor o menor número de puntos.

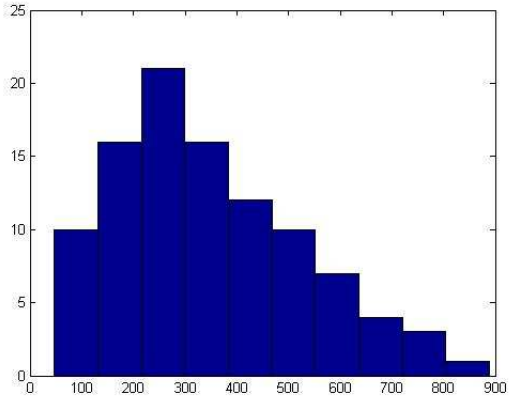


Figura 4.7: Puntos por usuario.

4.3.2 Complejidad de la firma / Puntos singulares

La complejidad de la firma se puede asemejar a la autenticación de los sistemas de rechazar a los usuarios que escogen PIN simples ya que son más fáciles de falsificar o forzar contraseñas que contienen caracteres en mayúsculas y minúsculas. Con la complejidad nos referimos a que una firma será más compleja cuando tenga muchos cambios en la misma, es decir, que no sea por ejemplo poner sólo su nombre y una raya que lo remarque.

Como medida de la complejidad utilizaremos el concepto de "stroke" y "punto singular" definidos en la norma ISO/IEC 19794-11 CD2[ISO09]. Los "puntos singulares" son aquellos puntos donde se produce un máximo o mínimo local de las señales X, Y y/o P. También se incluyen en los puntos singulares los "pen-down" (instante en el que el bolígrafo entra en contacto con la tableta) y los "pen-up" (instante en el que el bolígrafo deja de estar en contacto con la tableta). Se define un "stroke" como la porción de firma entre dos puntos singulares.

Mediante la función "strokes.m" y mediante una matriz en la que almacenamos el número de strokes por usuario, obtenemos el número de strokes de posición y

presión para cada firma de todos los usuarios. De nuevo utilizando estos datos, dividimos la base de datos en tres sub-bases de datos, para realizar una evaluación del rendimiento de los algoritmos para cada una de ellas.

- Aquellos con firmas no muy complejas (por debajo del percentil 25).
- Aquellos con firmas de complejidad alrededor de la media (entre el percentil 25 y el 75).
- Aquellos con firmas muy complejas (por encima del percentil 75).

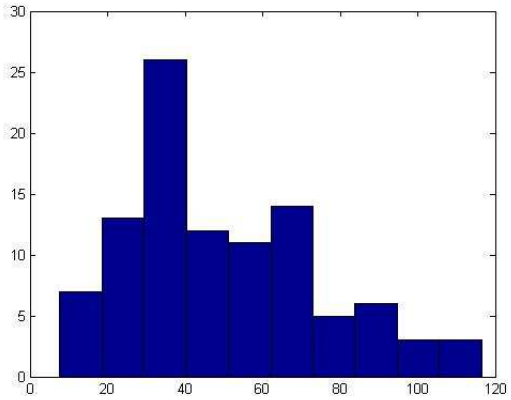


Figura 4.8: Puntos singulares (strokes) por usuario.

4.3.3 Coherencia de la firma

Es una parte muy importante a la hora de evaluar una firma. Nos permite saber cómo de variable es el usuario al firmar. Si el usuario cada vez que firma, firma de una manera distinta, la variabilidad es muy alta y por tanto la seguridad disminuye. Para tener una buena coherencia debemos tener una distribución normal a la hora de firmar. Con ello nos referimos a que cualquier característica dinámica de la firma sigue una distribución normal y además cualquier firma debe tener suficientes características dinámicas para poder asegurar la singularidad de la firma permitiendo así un buen proceso de verificación.

La coherencia de la firma es la más difícil de las mediciones de calidad para determinar, porque todo es una cuestión de equilibrio entre usabilidad y seguridad.

Para poder medir la coherencia de las firmas, nos hemos basado en calcular el número de puntos por firma así como la complejidad de la misma descritos anteriormente (véase apartados 4.3.1 y 4.3.2). Una vez que hemos calculado tanto los puntos como la complejidad de la misma, hemos obtenido su desviación típica. Basándonos en esta desviación típica, dividimos la base de datos en tres partes:

- Aquellos con firmas estables, baja desviación típica (por debajo del percentil 50).
- Aquellos con firmas no muy estables (entre el percentil 50 y el 75).
- Aquellos con firmas muy poco estables (por encima del percentil 75).

Esto división se hará tanto basándose en la desviación típica del número de puntos, como en la desviación típica del número de strokes.

La coherencia será hallada, gracias a la función “strokes.m” y “obtencionPuntos.m”.

Capítulo 5

Evaluación y Pruebas

En este capítulo nos presentamos los resultados de las evaluaciones para cada uno de los algoritmos que hemos descrito en el capítulo 3, GMM, DTW y DTW+GMM. Los resultados se dividen en varias partes, en la primera se analizará cada uno de ellos sin realizar ningún escalado a la base de datos, luego evaluaremos los algoritmos escalando las firmas para ver como afecta este escalado al rendimiento de los algoritmos. En la última parte analizaremos los tres aspectos indicados en el anexo B de la norma internacional ISO/IEC 19794-11 como indicadores del nivel de seguridad en la firma de un usuario.

5.1 Evaluación de los algoritmos de autenticación de firma manuscrita: DTW, GMM y DTW+GMM

La finalidad de este apartado es analizar cada uno de los algoritmos, es decir, queremos hallar las tasas de error de los tres algoritmos pero sin hacer ningún escalado en la base de datos de los 3 parámetros que se estudiarán con posterioridad: la posición, la presión y la frecuencia.

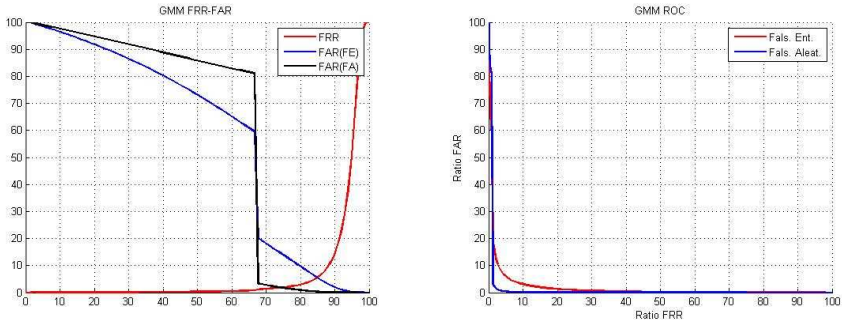
Para poder evaluarlos, se deben tener presentes los tres tipos de firmas que usamos en nuestra base de datos:

- Firmas genuinas: son las firmas originales de cada usuario.
- Firmas falsas entrenadas: son aquellas firmas que se han recogido cuando un usuario ha intentado suplantar a otro y ha tenido acceso al menos a una copia de la firma original a falsificar.
- Firmas falsas aleatorias: son aquellas firmas que se han recogido cuando un usuario ha intentado suplantar a otro sin tener conocimiento de la firma a falsificar. En nuestro caso se usarán las firmas genuinas de otros usuarios.

5.1.1 GMM

Factor de escala 0	
5.4640	EER_FE
1.8384	EER_FA

Tabla 5.1: Tasas de error del algoritmo GMM sin escalado.



(a) (b)

Figura 5.1: (a) Curva FRR-FAR del Algoritmo GMM sin escalado (b) Curva ROC del Algoritmo GMM sin escalado

Como podemos observar las tasas de error obtenidas (ver tabla 5.1) tanto con firmas falsas entrenadas como con las firmas falsas aleatorias son muy diferentes.

Con las graficas presentadas (ver figura 5.1) pretendemos visualizar dichas tasas de error. Mostramos la tasa de cruce, y como bien sabemos, cuánto menor sea el EER, tasa de error de cruce, más exacto es el sistema.

En nuestro caso, esta teoría no es muy aplicable ya no podemos hacer una comparativa de los valores obtenidos puesto que tenemos dos estudios diferentes. Debido a ello, las firmas falsas aleatorias deben tener un error mucho menor ya que la probabilidad de que las firmas se parezcan a la original son mínimas, mientras que en el caso de las firmas falsas entrenadas los errores son mayores debido a que tenemos un previo entrenamiento, sabemos o mejor dicho tenemos algo de conocimiento de cómo es la firma original.

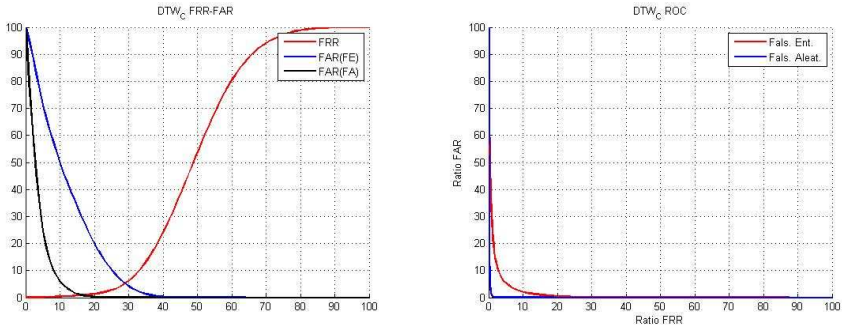
5.1.2 DTW

Factor de escala 0	
5.1831	EER_FE
0.8603	EER_FA

Tabla 5.2: Tasas de error del algoritmo DTW sin escalar.

En este caso obtenemos unas tasas de error del 5 % para firmas falsas entrenadas y menor del 1 % para firmas aleatorias (ver tabla 5.2).

Como hemos mencionado en el apartado anterior, los resultados obtenidos son lógicos ya que el error de las firmas falsas entrenadas es mucho mayor al de las falsas aleatorias.



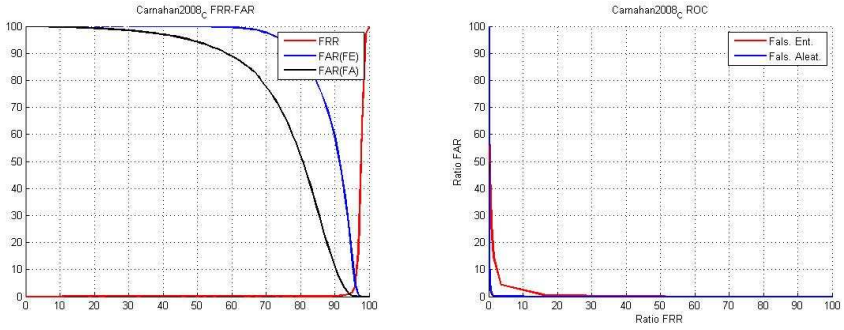
(a) (b)

Figura 5.2: (a) Curva FRR-FAR del algoritmo DTW sin escalar (b) Curva ROC del algoritmo DTW sin escalar

5.1.3 DTW+GMM

Factor de escala 0	
4.1455	EER_FE
0.9384	EER_FA

Tabla 5.3: Tasas de error del algoritmo GMM+DTW sin escalado.



(a) (b)

Figura 5.3: (a) Curva FRR-FAR del algoritmo GMM+DTW sin escalar (b) Curva ROC del algoritmo GMM+DTW sin escalar

Este algoritmo es el que mejores resultados tiene en cuanto a tasas de error. La tasa de error para firmas genuinas es un pelín superior al 4 %, mientras que las firmas aleatorias siguen estando por debajo del 1 % (ver tabla 5.3).

Hay que tener en cuenta, que estos tres algoritmos sólo utilizan la información capturada para las señales X, Y y presión.

5.2 Evaluación de los algoritmos aplicando a la resolución de los ejes X-Y, P y Frecuencia

EL objetivo de este apartado es analizar cada uno de los algoritmos, es decir, queremos hallar las tasas de error de los tres, pero en este caso haciendo el escalado de 3 parámetros posibles, la posición, la presión y la frecuencia de manera independiente. El escalado se hará con un factor de escala que toma valores de 1 a 6 en el caso de los ejes X e Y y la presión. Y valores de 1 a 4 para el caso de la frecuencia

5.2.1 Resolución X e Y

5.2.1.1 GMM

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
5.4664	5.4684	5.4282	5.4536	5.4635	5.6335	EER_FE
1.8365	1.7937	1.8561	1.7480	1.8002	1.8591	EER_FA

Tabla 5.4: Tasas de error del algoritmo GMM cuando escalamos la resolución.

Los resultados obtenidos para 6 factores de escala, son prácticamente iguales, no se aprecia apenas ninguna variación. Por lo que podemos concluir que la resolución de las tabletas gráficas no afecta notoriamente al rendimiento de este algoritmo (ver tabla 5.4).

En las dos primeras gráficas de la figura 5.4, se representa la curva ROC perteneciente a este algoritmo, donde cada curva pertenece a un escalado. Hemos querido representar también como es la curva del algoritmo si no hacemos ningún escalado para ver como variaban unas de otras. Para poder interpretar la gráfica, nos debemos fijar en el eje x e y pero justamente en la parte donde forman un ángulo de 90º. Cuanto más próxima este la curva de esa parte de los ejes, es mucho mejor.

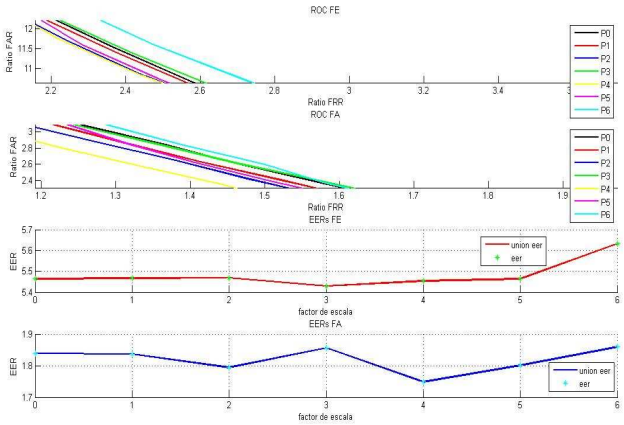


Figura 5.4: Curva ROC y Tasas de error del algoritmo GMM al escalar la resolución.

Las últimas dos graficas representan la tasa de error de cruce tanto para cuando usamos las firmas falsas aleatorias como firmas falsas entrenadas. Podemos observar que tenemos aproximadamente un 5 % y un 2 % de error medio respectivamente. Como se aprecia en estas dos últimas gráficas, la resolución de las tabletas gráficas no afecta al rendimiento de los algoritmos, manteniéndose las tasas de error en los mismos valores. Esto es debido a la alta resolución que poseen estos dispositivos (2000ppp).

5.2.1.2 DTW

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
5.1199	5.1085	5.0842	5.1068	5.1474	5.1568	EER_FE
0.8293	0.8397	0.8557	0.8631	0.8400	0.8543	EER_FA

Tabla 5.5: Tasas de error del algoritmo DTW cuando escalamos la resolución.

Los resultados obtenidos para 6 factores de escala, son prácticamente iguales, no se aprecia apenas ninguna variación. Por lo que podemos concluir que la resolución de las tabletas gráficas no afecta notoriamente al rendimiento de este algoritmo (ver tabla 5.5).

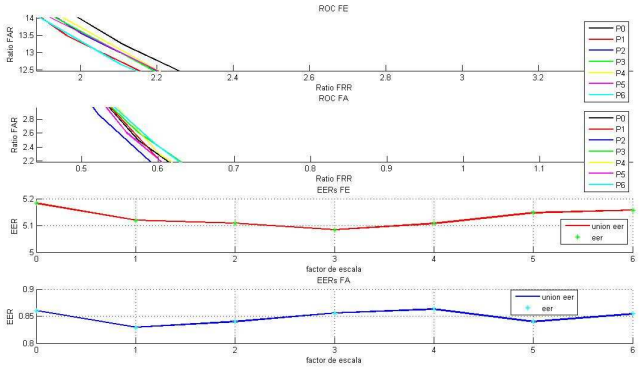


Figura 5.5: Curva ROC y Tasas de error del algoritmo DTW cuando escalamos la resolución.

Las últimas dos graficas (ver figura 5.5) representan la tasa de error de cruce tanto para cuando usamos las firmas falsas aleatorias como firmas falsas entrenadas. Podemos observar que tenemos aproximadamente un 5 % y un 1 % de error medio respectivamente. Las pequeñas oscilaciones que se ven entre las distintas resoluciones de los ejes X e Y probadas, son debidas a la dependencia estadística que tienen estas pruebas.

5.2.1.3 DTW+GMM

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
4.9085	4.5469	4.5373	4.7791	4.7458	4.4973	EER_FE
0.9898	0.9585	0.9758	0.9851	0.9691	0.9641	EER_FA

Tabla 5.6: Tasas de error del algoritmo GMM+DTW cuando escalamos la resolución.

De nuevo, para este algoritmo también volvemos a obtener que la resolución de los ejes X-Y no afecta al rendimiento (ver tabla 5.6).

De nuevo, las pequeñas oscilaciones que se ven entre las distintas resoluciones de los ejes X e Y probadas, son debidas a la dependencia estadística que tienen estas pruebas (ver figura 5.6).

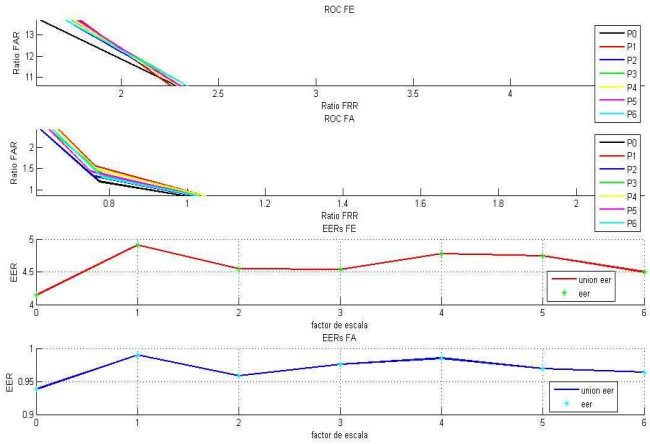


Figura 5.6: Curva ROC y Tasas de error del algoritmo GMM+DTW cuando escalamos la resolución.

5.2.2 Resolución de la presión

5.2.2.1 GMM

De nuevo, podemos comprobar que en la precisión a la hora de captura, la presión no aporta una información definitiva cuando realizamos la autenticación de usuarios a través de la firma manuscrita (ver tabla 5.7).

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
5.4718	5.5036	5.4941	5.6574	5.6866	5.7988	EER_FE
1.8435	1.8474	1.8211	1.8055	1.8399	1.8325	EER_FA

Tabla 5.7: Tasas de error del algoritmo GMM cuando escalamos la presión.

Si se puede apreciar una pequeña pendiente, que indica una pérdida de rendimiento. Pero esta perdida es bastante pequeña si la comparamos con la diferencia de precisión a la hora de medir las presiones entre la resolución inicial (1024-0) y la resolución del escalado 6 (16-0) (ver figura 5.7).

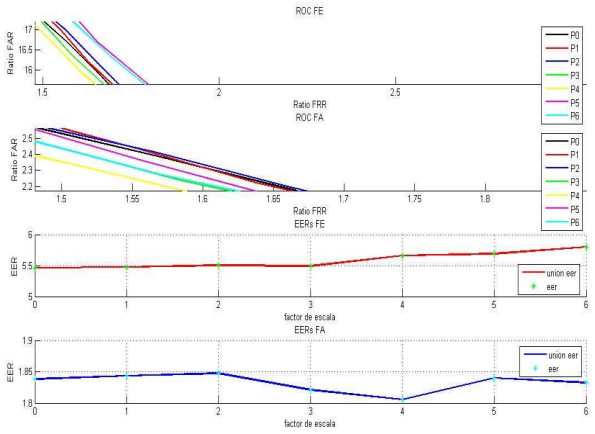


Figura 5.7: Curva ROC y Tasas de error del algoritmo GMM cuando escalamos la presión.

5.2.2.2 DTW

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
5.0843	5.1250	5.1249	5.1025	5.1094	5.0400	EER_FE
0.8413	0.8347	0.8538	0.8482	0.8316	0.8291	EER_FA

Tabla 5.8: Tasas de error del algoritmo DTW cuando escalamos la presión.

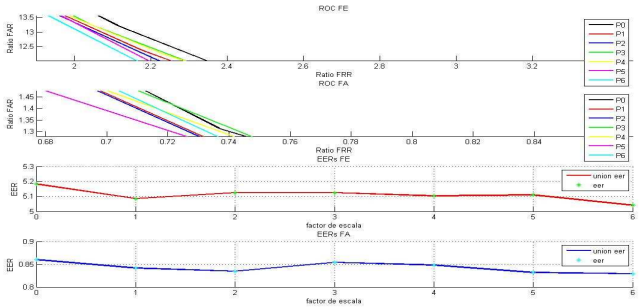


Figura 5.8: Curva ROC y Tasas de error del algoritmo DTW cuando escalamos la presión.

En este caso, los resultados obtenidos son similares al anterior algoritmo, exceptuando que no se aprecia la pendiente creciente al bajar la resolución de captura de la presión (ver figura 5.8). Esto indica que este algoritmo es más robusto frente a la precisión de captura de la presión que el algoritmo anterior.

5.2.2.3 DTW+GMM

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	Factor escala 5	Factor escala 6	
4.8520	4.7137	4.7083	4.8321	4.7685	4.6773	EER_FE
0.9855	0.9501	0.9726	0.9636	0.9735	0.9781	EER_FA

Tabla 5.9: Tasas de error del algoritmo GMM+DTW cuando escalamos la presión.

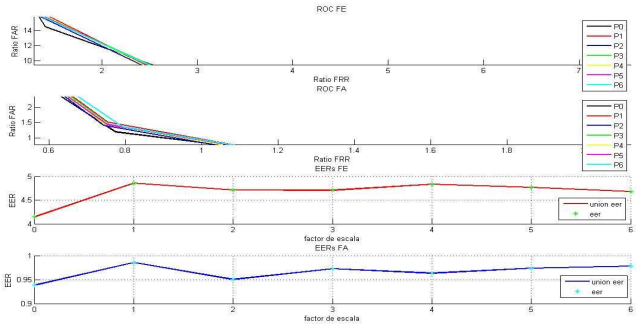


Figura 5.9: Curva ROC y Tasas de error del algoritmo GMM+DTW cuando escalamos la presión.

Como se puede apreciar en las gráficas (ver figura 5.9), este algoritmo se muestra también robusto frente a las distintas resoluciones de captura de la presión probadas.

Como resultado de estas evaluaciones, de nuevo cabe destacar la poca importancia en la resolución de captura de la presión. Una gran resolución de captura no aporta ninguna ventaja en el rendimiento de los algoritmos. Este hecho nos permitiría utilizar dispositivos de bajo coste en aquellos sistemas donde se pensará utilizar estos algoritmos para la autenticación de usuarios.

Eso si, hay que recordar que la captura de la presión nos aporta una información muy importante para el buen funcionamiento de los algoritmos, pero con este estudio se ha demostrado que su captura no tiene por ser de una gran resolución.

5.2.3 Resolución de la frecuencia

5.2.3.1 GMM

En el caso de la resolución de muestreo de las tabletas gráficas, esta frecuencia si que tiene un fuerte impacto en el rendimiento de los algoritmos (ver tabla 5.10).

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	
6.0496	6.9366	8.4212	11.8708	EER_FE
2.1531	3.0912	4.1920	6.4059	EER_FA

Tabla 5.10: Tasas de error del algoritmo GMM cuando escalamos la frecuencia.

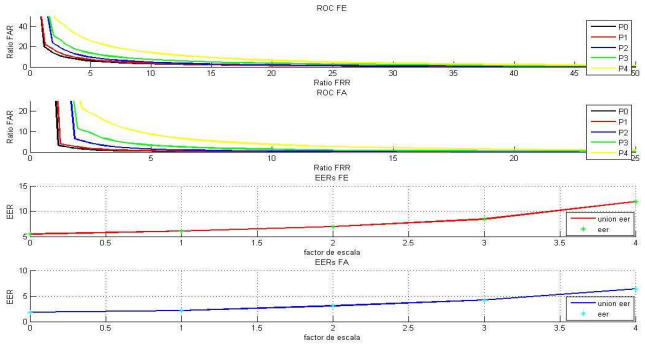


Figura 5.10: Curva ROC y Tasas de error del algoritmo GMM cuando escalamos la frecuencia.

En las dos última gráficas (ver figura 5.10), se puede observar como según disminuye la frecuencia de muestreo (100,50,25 y 12 Hz respectivamente) la tasas de errores, tanto para las firmas falsificadas entrenadas como para las firmas aleatorias, aumenta de manera notable.

5.2.3.2 DTW

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	
5.1912	5.2583	6.3895	13.5300	EER_FE
0.8755	0.8821	1.0938	3.8906	EER_FA

Tabla 5.11: Tasas de error del algoritmo DTW cuando escalamos la frecuencia.

Este algoritmo, comparado con el anteriormente evaluado, se muestra más robusto frente a la frecuencia de muestreo de las muestras, ya que hasta que no alcanzamos una frecuencia de 12,5 Hz, las tasas de error se habían mantenido aproximadamente estables. Como se aprecia en la figura 5.11, para un escalado de 4 (frecuencia de muestro 12,5 hz) las tasas de error aumentan considerablemente.

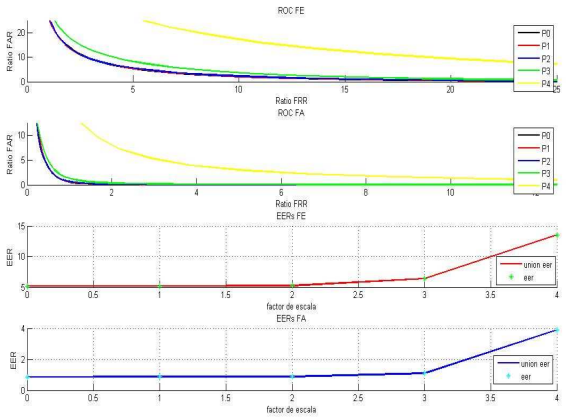


Figura 5.11: Curva ROC y Tasas de error del algoritmo DTW cuando escalamos la frecuencia.

5.2.3.3 DTW+GMM

Factor escala 1	Factor escala 2	Factor escala 3	Factor escala 4	
4.5781	4.6896	6.3338	12.8806	EER_FE
0.9585	0.9902	1.0523	3.9120	EER_FA

Tabla 5.12: Tasas de error del algoritmo GMM+DTW cuando escalamos la frecuencia.

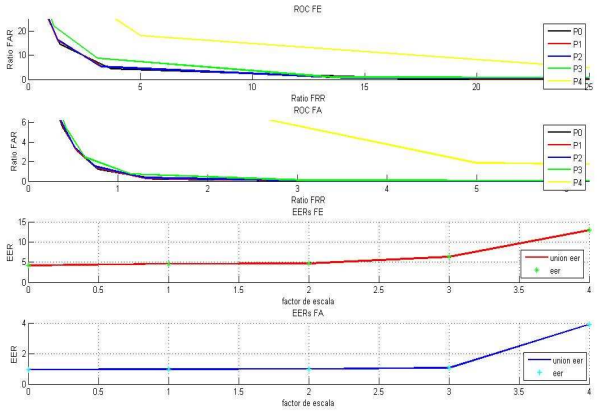


Figura 5.12: Curva ROC y Tasas de error del algoritmo GMM+DTW cuando escalamos la frecuencia.

Los resultados de este algoritmo son muy similares al anterior, mostrándose robusto frente a la frecuencia de muestreo, hasta alcanzar el factor de escalado 4.

5.3 Evaluación de la importancia del número de puntos de una firma en el rendimiento de los algoritmos

Este apartado tiene como finalidad evaluar el impacto del número de puntos de la firma de un usuario en el rendimiento de los algoritmos. Como sugiere la [norma ISO/IEC 19794-11 Anexo B], se espera que una mayor cantidad de puntos implique una mayor seguridad de la firma. Cuanto más puntos tenga la firma, más complicado debería ser flasificarla. Una vez obtenido los puntos medios de las firmas por usuarios, se ha dividido nuestra base de datos en tres sub-bases. Aquellos usuarios que tienen una media de puntos por debajo del percentil 25, los que se encuentran entre el percentil 25 y el 75, y finalmente, aquellos que se encuentran por encima del 75. Evaluaremos cada una de las bases de datos basándonos en los tres algoritmos, GMM, DTW y Gmm+DTW. Otro aspecto que se va a evaluar en la consistencia en realizar la firma. Esto lo obtendremos a partir de la desviación típica del número de puntos de cada usuario. Aquellos usuarios que mantienen el número de puntos al firmas más estable, deberían tener unas tasas de error mejores que aquellos que tienen una desviación típica alta, ya que estos introducen una mayor variabilidad en su firma que puede ser utilizada en su favor por los falsificadores. La división en este caso se ha realizado creando una primera sub-base de datos con aquellos usuarios que tienen una desviación típica por debajo del percentil 50, otra con aquellos que se encuentran entre el 50 y el 75, y la última con aquellos que superan el percentil 75.

La base de datos se ha dividido de la siguiente manera, atendiendo a los dos aspectos comentados:

- Puntos medios

BBDD Inferior	BBDD Central	BBDD Superior
1x26	1x49	1x25

Tabla 5.13: División de la base de datos según los puntos medios.

- Desviación típica de los puntos medios

BBDD Inferior	BBDD Central	BBDD Superior
1x50	1x25	1x25

Tabla 5.14: División de la base de datos de la desviación típica de los puntos medios.

Pretendemos evaluar cada una de nuestras subdivisiones de la base de datos y obtener tanto los umbrales, la tasa de error (EER) como la ROC.

Para la evaluación debemos tener en cuenta que cuanto más puntos tengan las firmas más difíciles serán de falsificar, por lo que las tasas de error deberían ser mayores para aquella base de datos que contenga usuarios con firmas muy cortas (base inferior), seguida de la base de datos que contenga usuarios con firmas de tamaño medio (base central) y por último la base de datos que contenga a usuarios de firmas con muchos puntos (base superior). Por tanto se espera que esta última sea la que tenga las mejores tasas.

Por otro lado, al evaluar la desviación típica de los puntos, debemos tener en cuenta, que a mayor desviación tendremos firmas con mayor probabilidad de falsificación. Como consecuencia, esperamos que la mayor tasa de error la tenga la base de datos que tenga mayor desviación típica.

5.3.1 GMM

5.3.1.1 Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
8.3032	4.2773	4.8980	EER_FE
2.7602	2.5168	1.9291	EER_FA

Tabla 5.15: Tasas de error de los puntos medios del algoritmo GMM.

Los resultados obtenidos, reflejan que la base de datos inferior si analizamos primero el uso de firmas falsas entrenadas, tiene un error mucho mayor aproximadamente de un 8 %. Esto es debido a que los usuarios pertenecientes a esta base de datos serán aquellos a los que se les pueda falsificar la firma fácilmente, serán aquellos que a la hora de registrar sus firmas han firmado de manera muy rápida por lo que no se ha podido coger toda la información necesaria sobre las mismas. Ocurriría lo mismo con el uso de las firmas falsas aleatorias, la tasa de error esta entorno un 3 % en la base de datos inferior.

Esto indica que las firmas cortas no aportan la información necesaria para realizar una buena autenticación de usuario, en sistemas donde la seguridad sea algo crítico, se debería limitar el número de puntos inferior de las firmas, para evitar posibles usos fraudulentos.

La diferencia entre la base de datos central y superior no es muy notable, de donde se puede extraer la conclusión que una gran cantidad de puntos tampoco implica una mayor seguridad en la firma del usuario.

5.3.1.2 Desviación Típica de los Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
4.7701	6.4010	5.8614	EER_FE
1.4231	2.2833	2.2268	EER_FA

Tabla 5.16: Tasas de error de la desviación típica de los puntos medios del algoritmo GMM.

Los resultados obtenidos demuestran también la importancia en la variabilidad de la firma. Los usuarios con una menor desviación típica obtienen unos resultados mucho mejores, como era de esperar, que aquellos que firman de una manera mucho más inestable.

También se puede apreciar que no existe una gran diferencia en cuanto a rendimiento entre la base de datos central y la superior, por lo que una vez que la firma es suficientemente inestable, una mayor inestabilidad no afecta muy negativamente al rendimiento del algoritmo.

De nuevo, en el caso de utilizar este algoritmo de autenticación en entornos donde la seguridad sea una prioridad, se debería indicar a los usuarios la importancia de tener una firma lo mas estable posible, y en caso de no ser así, se podría llegar a rechazar la inclusión de esos usuarios, ya que podrían generar un agujero de seguridad en el sistema.

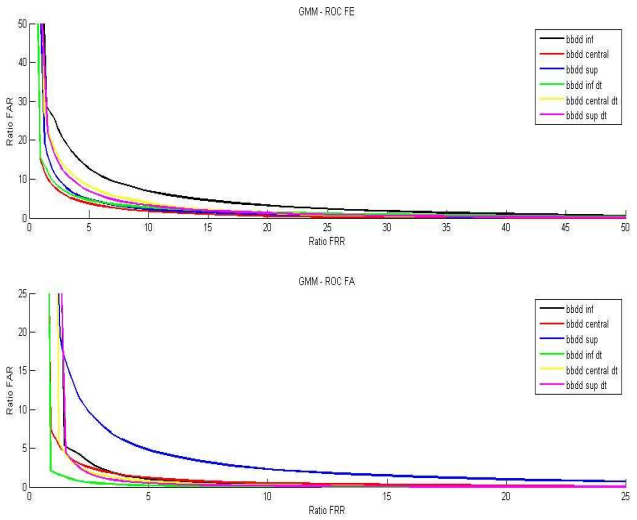


Figura 5.13: Curva ROC de los puntos medios y desviación típica del algoritmo GMM.

Las gráficas representan la curva ROC tanto para las firmas falsas entrenadas como para las firmas falsas aleatorias. Si nos centramos en la primera gráfica, observamos 6 curvas ROC, cada una de ellas pertenecientes a las sub-bases obtenidas

anteriormente, tanto para las sub-bases de números de puntos y las sub-bases de desviación típica. Ocurriría lo mismo en la segunda gráfica (ver figura 5.13).

5.3.2 DTW

5.3.2.1 Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
7.1511	4.1345	4.6531	EER_FE
0.8879	0.8202	1.0362	EER_FA

Tabla 5.17: Tasas de error de los puntos medios del algoritmo DTW.

Para el algoritmos DTW obtenemos unos resultados similares al algoritmo anterior. En el caso de falsificaciones entrenadas, la tasa de error de las firmas con un menor número de puntos es mucho mayor que el resto, sin existir una gran diferencia entre la base de datos central e inferior.

Sin embargo, este algoritmo se muestra mucho mas robusto en este aspecto para las firmas aleatorias, ya que no existen grandes diferencias para ninguna de las tres bases de datos.

5.3.2.2 Desviación Típica de los Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
3.8551	6.4739	6.2599	EER_FE
0.2753	1.4908	1.6637	EER_FA

Tabla 5.18: Tasas de error de la desviación típica de los puntos medios del algoritmo DTW.

En este caso, se ve claramente lo importante de realizar una firma estable para evitar falsificaciones. La diferencia en cuanto a las tasas de error es bastante importante entre aquellos usuarios con una baja desviación típica y el resto.

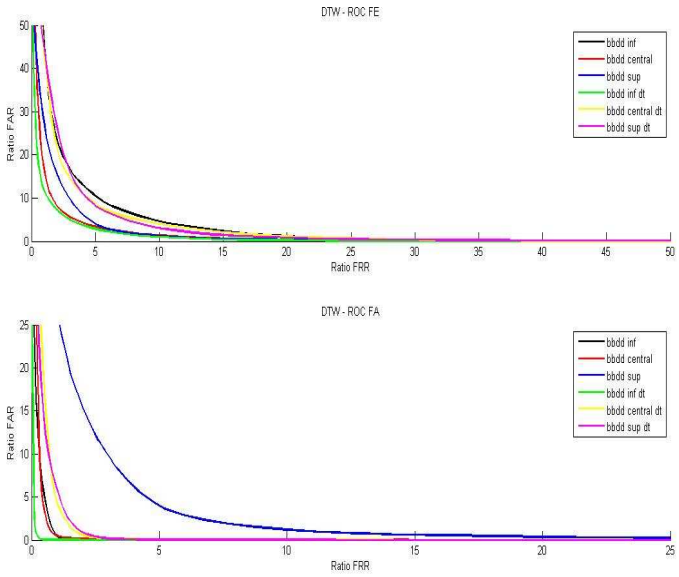


Figura 5.14: Curva ROC de los puntos medios y desviación típica del algoritmo DTW.

Las gráficas representan la curva ROC tanto para las firmas falsas entrenadas como para las firmas falsas aleatorias. Si nos centramos en la primera gráfica, observamos 6 curvas ROC, cada una de ellas pertenecientes a las sub-bases obtenidas anteriormente, tanto para las sub-bases de números de puntos y las sub-bases de desviación típica. Ocurriría lo mismo en la segunda gráfica (ver figura 5.14).

5.3.3 DTW+GMM

5.3.3.1 Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
6.3885	3.8642	4.7532	EER_FE
0.9333	0.9266	1.0729	EER_FA

Tabla 5.19: Tasas de error de los puntos medios del algoritmo GMM+DTW.

Los resultados y las conclusiones son similares a los obtenidos con el algoritmo anterior.

5.3.3.2 Desviación Típica de los Puntos Medios

BBDD Inferior	BBDD Central	BBDD Superior	
3.7068	6.4027	5.9024	EER_FE
0.3087	1.5235	1.6154	EER_FA

Tabla 5.20: Tasas de error de la desviación típica de los puntos medios del algoritmo DTW+GMM.

Los resultados y las conclusiones son similares a los obtenidos con el algoritmo anterior.

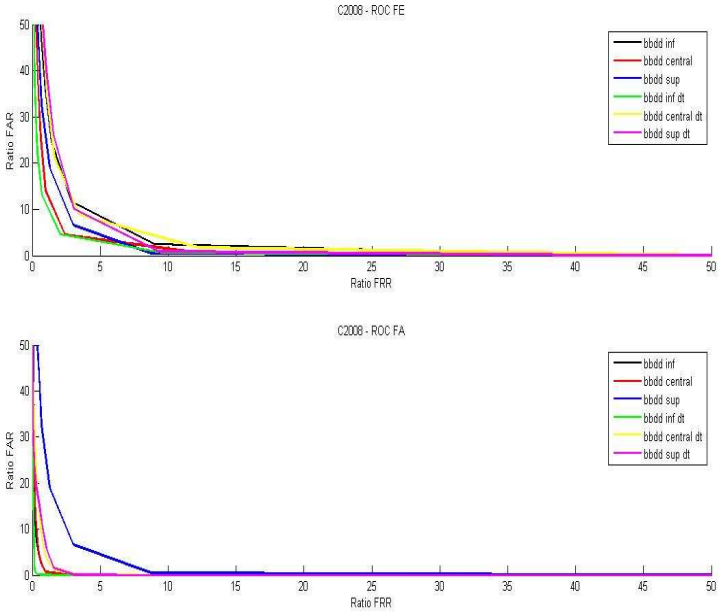


Figura 5.15: Curva ROC de los puntos medios y de la desviación típica del algoritmo DTW+GMM.

Las gráficas representan las curvas ROC para cada una de las sub-bases obtenidas anteriormente (ver figura 5.15).

5.4 Evaluación de la importancia del número de puntos singulares (strokes) de una firma en el rendimiento de los algoritmos

Como hemos visto en el apartado anterior, cuando evaluábamos la cantidad de puntos por usuario, juega un papel importante si poseen mucha cantidad o no. Pero en este apartado evaluamos algo aún si cabe más importante aún, vamos a ver la importancia que juega el hecho de que un usuario tenga una firma más compleja que otro. La complejidad de la firma la mediremos con el número de puntos singulares (definidos en la norma ISO/IEC 19794-11). También, de nuevo, estudiaremos la estabilidad de los usuarios al realizar la firma utilizando la desviación media del número de puntos singulares. En la división de las base de dato se usaran los mismos criterios que el anterior apartado.

A continuación, se muestra el número de usuarios en cada subdivisión de la base de datos:

- Número medio de strokes

BBDD Inferior	BBDD Central	BBDD Superior
1x22	1x52	1x26

Tabla 5.21: División de la base según el número medio de strokes.

- Desviación típica del número de strokes

BBDD Inferior	BBDD Central	BBDD Superior
1x50	1x25	1x25

Tabla 5.22: División de la base según la desviación típica del número de strokes.

Pretendemos evaluar cada una de nuestras subdivisiones de la base de datos y obtener tanto los umbrales, la tasa de error (EER) como la ROC.

Para la evaluación debemos tener en cuenta ciertos aspectos como a la hora de evaluar la cantidad de puntos.

Cuanto mayor sea el número de strokes o puntos singulares, más difíciles serán de falsificar las firmas, por lo que las tasas de error deberían ser mayores para aquella base de datos que contenga usuarios con firmas menos complejas (base inferior), seguida de la base de datos que contenga usuarios con firmas de complejidad media (base central) y por ultimo la base de datos que contenga a usuarios de firmas mas complejas (base superior). Por tanto se espera que esta última sea la que tenga las mejores tasas.

Por otro lado, al evaluar la desviación típica de los puntos singulares, debemos tener en cuenta, que a mayor desviación tendremos firmas con mayor probabilidad de falsificación. Como consecuencia, esperamos que la mayor tasa de error la tenga la base de datos que tenga mayor desviación típica.

5.4.1 GMM

5.4.1.1 Puntos Singulares/Strokes medios

BBDD Inferior	BBDD Central	BBDD Superior	
8.2696	4.2118	4.9963	EER_FE
2.2385	2.2960	1.9083	EER_FA

Tabla 5.23: Tasas de error de los puntos singulares del algoritmo GMM.

Observamos como el resultado es muy similar al obtenido con respecto al número de puntos medios del usuario. La base de datos inferior tiene unas tasas de error muy superiores con respecto a las otras (teniendo en cuenta las firmas falsas entrenadas). De nuevo esta diferencia no se aprecia entre la base de datos central y la superior (ver tabla 5.23).

5.4.1.2 Desviación típica de los strokes

BBDD Inferior	BBDD Central	BBDD Superior	
3.8007	5.7455	6.2904	EER_FE
0.4796	1.4252	1.6122	EER_FA

Tabla 5.24: Tasas de error de la desviación típica los puntos singulares del algoritmo GMM.

En este caso, obtenemos unos resultados bastante extraños, ya que la mayor variabilidad en el número de puntos, no implica una mayor facilidad para la falsificación.

Esto se puede explicar debido a que existe una gran variabilidad a la hora de calcular los puntos singulares, que son muy sensibles al ruido introducido por el sensor a la hora de capturar las señales de X e Y, y especialmente en el caso de la señal de presión.

Estas pruebas se deberían repetir para la nuevo versión del estándar que se esta realizando, en la cual se espera se solucioné este problema.

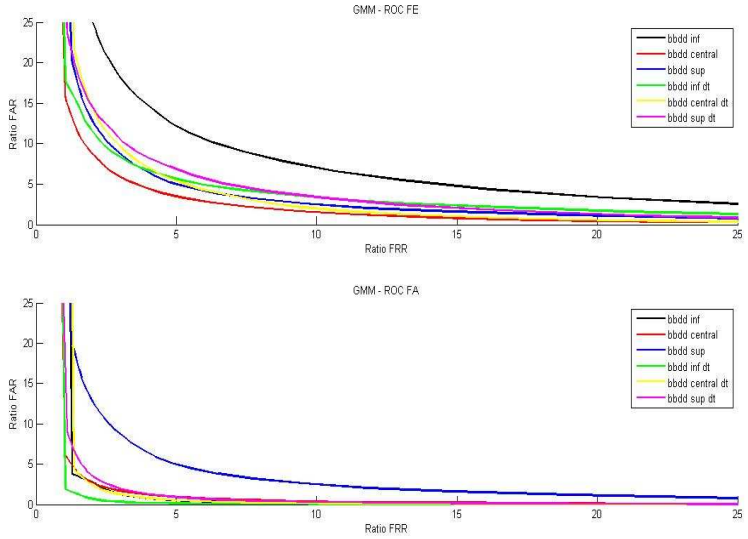


Figura 5.16: Curva ROC de los puntos singulares y la desviación típica del algoritmo GMM.

En las gráficas anteriores(ver figura 5.16), observamos las diferentes curvas ROC para cada una de las sub-bases obtenidas.

5.4.2 DTW

5.4.2.1 Puntos Singulares/Strokes medios

BBDD Inferior	BBDD Central	BBDD Superior	
6.4367	4.4610	5.1485	EER_FE
0.5763	0.9509	1.1079	EER_FA

Tabla 5.25: Tasas de error de los puntos singulares del algoritmo DTW.

Observamos de nuevo un comportamiento similar al caso anterior, aunque en este caso, este algoritmos se muestra mas sensible al número de puntos singulares para falsificaciones con firma aleatorias. Este algoritmo se muestra, de nuevo, más robusto que el anterior.

5.4.2.2 Desviación típica de los strokes

BBDD Inferior	BBDD Central	BBDD Superior	
4.0033	6.2413	6.2599	EER_FE
0.4802	1.2601	1.6637	EER_FA

Tabla 5.26: Tasas de error de la desviación típica de los puntos singulares del algoritmo DTW.

Los resultodos en este caso, si muestran una tendencia a que aquellos usuarios con una menor desviación típica obtengan unas tasas de error mejores. Aún así, la diferencia sigue siendo mucho menor que en el caso de tener en cuenta el número de puntos.

Las gráficas (ver figura 5.17) nos reflejan las curvas ROC para cada una de las sub-bases tanto para el caso de los strokes medios y la desviación típica de los mismos.

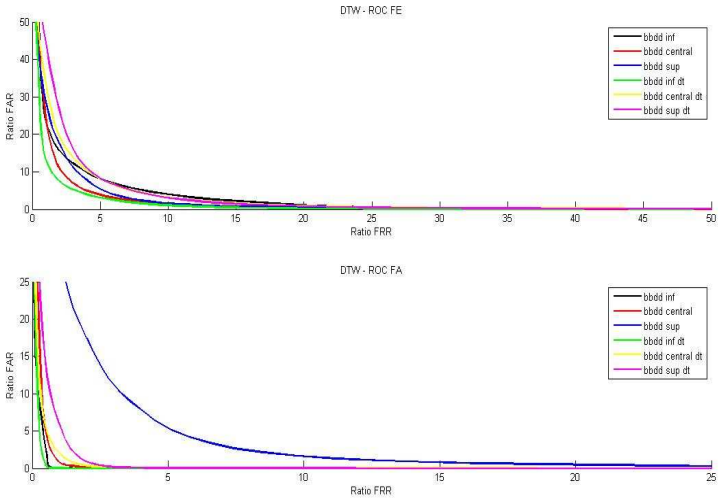


Figura 5.17: Curva ROC de los puntos singulares y la desviación típica del algoritmo DTW.

5.4.3 DTW+GMM

5.4.3.1 Puntos Singulares/Strokes medios

BBDD Inferior	BBDD Central	BBDD Superior	
5.8070	4.2204	4.9671	EER_FE
0.6587	1.0552	1.0571	EER_FA

Tabla 5.27: Tasas de error de los puntos singulares del algoritmo DTW+GMM.

Para este algoritmo, se sigue mostrando un peor rendimiento en la base de datos inferior, aunque la diferencia es mucho menor que en los algoritmo anteriores. Este algoritmos es el que se ha mostrado más robusto de los tres, discriminando mucho las falsificaciones, independientemente del número de puntos singulares de cada usuario.

5.4.3.2 Desviación típica de los strokes

BBDD Inferior	BBDD Central	BBDD Superior	
3.8007	5.7455	6.2904	EER_FE
0.4796	1.4252	1.6122	EER_FA

Tabla 5.28: Tasas de error de los puntos singulares del algoritmo DTW+GMM.

De nuevo, vemos como aquellos usuarios que muestran una menor desviación típica en el número de puntos singulares, son aquellos que obtienen las mejores tasas de errores. También, de nuevo, estas diferencias no son tan marcadas como en el caso de la desviación típica de los números de puntos muestreados, que se puede explicar por lo comentado sobre la inestabilidad a la hora de calcular los puntos singulares.

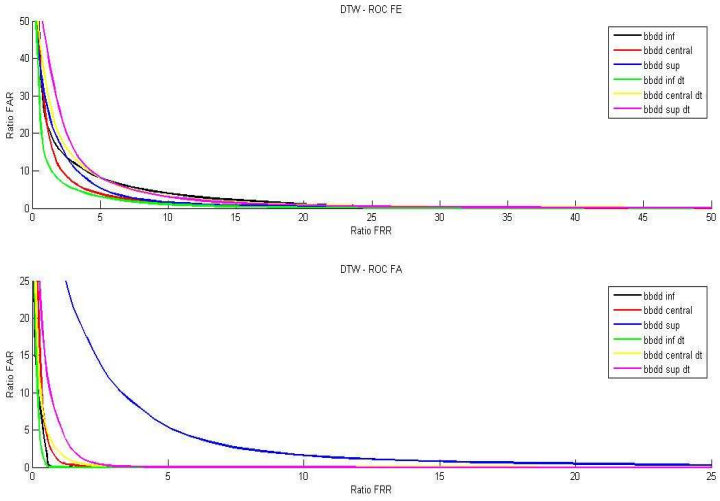


Figura 5.18: Curva ROC de los puntos singulares y la desviación típica del algoritmo DTW+GMM.

Las gráficas (ver figura 5.18) nos muestran las curvas ROC para cada una de las sub-bases tanto para el caso de los puntos medios y la desviación típica de los mismos.

Capítulo 6

Conclusiones y Trabajos Futuros

En este capítulo nos centraremos en expresar las conclusiones a las que hemos llegado al obtener los resultados y los posibles trabajos futuros.

6.1 Conclusiones

La biometría es una técnica madura que posee numerosas aplicaciones. Es una técnica robusta, ofreciendo algunas de sus modalidades (por ejemplo iris y huella dactilar) una gran fiabilidad. Sin embargo, en nuestro caso específico de firma manuscrita posee un gran riesgo de falsificación. Aún así, la firma manuscrita, teniendo en cuenta su enorme ámbito de utilidad y su gran aceptación por los usuarios, es una técnica que no solamente está asociada a temas de seguridad sino también entornos de detección de fraude, como por ejemplo todo tipo de transacciones comerciales (como por ejemplo la utilización de tarjetas bancarias).

El presente proyecto, trata de implementar un método de evaluación basado en el proyecto ISO/IEC 19785 para realizar evaluaciones de algoritmos de firma manuscrita. Esta implementación se probará a través de tres algoritmos: GMM, DTW y DTW+GMM, con el fin de ver con cual de ellos obtenemos mejores resultados en cuanto a tasas de error se refiere, así como evaluar como el grado de resolución en la captura de las señales que conforman la firma manuscrita (ejes X e

Y, presión y frecuencia de muestreo) afectan al rendimiento de estos algoritmos.

En la primera parte de este proyecto se ha evaluado los algoritmos por separado y sin modificar la base de datos de referencia (MCyT Signature Database). Los resultados obtenidos han mostrado como el algoritmo que combina DTW y GMM consigue los mejores resultados en cuanto a tasas de error (EER): 4.14 % en la detección de firmas falsificadas entrenadas, siendo del 0.93 % para firmas falsas aleatorias. Los resultados obtenidos son los que esperábamos ya que tenemos tasas de errores mayores al analizar las firmas falsas entrenadas que en las firmas falsas aleatorias. Estos resultados tienen su lógica ya que las firmas falsas entrenadas han sido recogidas para usarlas en nuestras base de datos con un previo ensayo, es decir, el usuario poseía el conocimiento de cómo es la firma original y pudo practicarla, por lo que la tasa de error debe ser mayor que si la comparamos con la tasa de error obtenida para las firmas falsas aleatorias que han sido recogidas sin que el usuario tuviera conocimiento alguno.

A continuación se ha evaluado cada uno de los algoritmos pero aplicando distintas resoluciones a las señales de los ejes X e Y, de la presión y a la frecuencia de muestro de la base de datos de referencia (MCyT). Se observada que al escalar tanto la posición como la presión no se obtienen perdidas significativas en el rendimiento de los algoritmos evaluados, algo que no esperábamos pues al escalar los parámetros se pierde precisión en la captura de la firma manuscrita. Esto indica que la resolución de captura del dispositivo utilizado para obtener la base de datos MCyT (Wacom Intous 2) tiene unas características de resolución para estas tres señales (ejes X-Y y Presión) mucho mayores de los necesarios para realizar una correcta autenticación de firma manuscrita. Esta tableta es una de las tabletas más avanzadas, y por ello de mayor coste, con lo que a través de estos resultados podemos concluir que la utilización de tabletas con menores resolución de captura para estos parámetros, además de un menor coste, no afecta al rendimiento de los sistemas de autenticación de firma manuscrita.

Por lo contrario, al escalar la frecuencia, observamos en los tres algoritmos, que a medida que vamos aumentando el factor de escala, el error va incrementándose

también. Por lo tanto, se comprueba que la frecuencia de muestreo si que es un factor importante a la hora de decidir que dispositivo de captura utilizar, no siendo recomendable utilizar dispositivos de captura con frecuencia de muestro menor de 50 Hz, y en ningún caso debería ser aceptable utilizar dispositivos con frecuencias menores de 25 Hz, a partir de las cuales las tasas de errores crecen muy significativamente.

En la segunda parte del proyecto, nos centrábamos en evaluar el impacto de ciertos parámetros en la seguridad de la firma de los usuarios, parámetros sugeridos en el Anexo B de la norma ISO/IEC 19794-11. En particular se han analizado la cantidad de puntos por cada firma como indicador de la cantidad de información, la cantidad de strokes o puntos singulares como indicador de la complejidad de la firma. También se han evaluado la variabilidad de estos parámetros como indicadores de al estabilidad de la firma de cada usuario.

Como se ha citado en el apartado 5.3 y 5.4, se esperaba que las tasas de error fueran mayores en el caso de que el número de puntos o el número de strokes fuesen mayores. Por consiguiente, esperábamos que la tasa de error mayor estuviese en la base de datos con usuarios con firmas muy cortas, seguida de firmas de tamaño medio y por último la base con firmas de tamaño elevado.

En el caso del número medio de puntos de la firma de cada usuario (cantidad de información) se ha observado, para las firmas falsas entrenadas, que se cumple especialmente para el caso de la sub-base de datos inferior (aquella con las firmas con un menor número de puntos, obteniendo unas tasas de errores mucho mayores que para las otras dos partes de, mientras que las otras dos sub-bases de datos obtienen unos resultados muy similares, aunque sorprende que se obtengan resultados ligeramente peores para las firmas con mas puntos. Esto puede deberse a que al tener un mayor número de puntos las firmas son menos estables. Este comportamiento se observa para los tres algoritmos estudiados. Este comportamiento es distinto para las tasas de error con firmas aleatorias donde las diferencias no son muy significativas entre las distintas bases de datos.

En el caso de la desviación típica (estabilidad de la firma) también los resultados son aproximadamente los esperados. Para firmas falsas entrenadas, aquella base de datos (inferior) con una menor desviación típica es la que obtiene una menor tasa de error, al ser la firma más estable. De nuevo, las diferencias entre la base de datos central y la superior no son muy notables. En el caso de las firmas falsas aleatorias, si que se muestra una gran reducción de la tasas de error en la base de datos con menor desviación típica, mostrando que estas firmas son mucho más robustas frente a este tipo de falsificaciones.

6.2 Trabajos futuros

Los trabajos futuros que se plantean para este proyecto se citan a continuación:

- Incluir en los estudios las señales de inclinación (elevación y altitud) proporcionadas por las tabletas digitales. Realizar de nuevo una evaluación sobre el impacto de la resolución de la captura de estas señales en el rendimiento de los algoritmos
- Implementar las pruebas en C, para aumentar la rapidez de ejecución, ya que la ejecución en matlab de evaluación completa de cada uno de los algoritmos es demasiado lento.
- Implementar los algoritmos en C también para mejorar la velocidad en la evaluación de los algoritmos.
- Estudiar técnicas de selección de características para mejorar el rendimiento de los algoritmos (PCA, ICA, Fisher...)
- Estudiar los intervalos de confianza para cada uno de los algoritmos.
- Crear una interface gráfica para realizar las evaluaciones, que permite controlar todos los parámetros necesarios (número de simulaciones, número de firmas a utilizar: genuina, falsas, aleatorias).

- Creación automática de un documento de resultados con toda la información necesaria.

Bibliografía

[A.k99] S.Pankanti A.k.Jain, R.Bolle. Face recognition. In *In Biometrics: Personal Identification in Networked Society*, pages 65–86. Kluwer Academic Publishers, 1999.

[And03] Jonas Richiardi And. Gaussian mixture models for on-line signature verification, 2003.

[Bil98] Jeff Bilmes. A gentle tutorial of the em algorithm and its application to parameter estimation for gaussian mixture and hidden markov models. Technical report, 1998.

[Dau93] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. Pattern Anal. Mach. Intell.*, 15(11):1148–1161, 1993.

[G.R] G.R.Doddington. Speaker recognition-identifying people by their voice. Proceeding of the IEEE, vol.73, nº11, Nov. 1985.

[ISO05] Iso/iec19795-1, 2005. information technology-biometric performance testing and reporting-part 1: Principles and framework. iso/iec jtc1/sc37 n908., 2005. .

[ISO06] Iso/iec 19795-2, 2006.biometric performance testing and reporting. part 2: Testing methodologies for technology and scenario evaluation., 2006. .

[ISO09] Iso/iec 19794-11, 2009.signature/sign processed dynamic data. anexo b, 2009. .

[LT99] S. B. Lee and S. Tsutsui. *Intelligent biometric techniques in fingerprint and face recognition.* CRC Press, Inc., Boca Raton, FL, USA, 1999.

[MWD+02] A. J. Mansfield, J. L. Wayman, Authorised Dr, Dave Rayner, and J. L. Wayman. Best practices in testing and reporting performance, 2002.

[O.] O. Miguel-Hurtado, L. Mengibar-Pozo, M.G. Lorenz, J. Lui-Jimenez. On-line signature verification by dynamic time warping and gaussian mixture models. IEEE Tans. Int. Carnahan Conf. on Security Technology, 2007.

[O. 07a] O. Miguel-Hurtado, L. Mengibar-Pozo, Andrzej Pacut. A new algorithm for signature verification system based on dtw and gmm, 2007. .

[O. 07b] O. Miguel-Hurtado, L. Mengibar-Pozo, Sanchez-Reillo. On-line signature biometrics with gmm and minimal vector size, 2007. Preprint submited to Elsevier, Agosto 2007.

[RQD00] Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. Speaker verification using adapted gaussian mixture models. In *Digital Signal Processing*, page 2000, 2000.

[R.Sa] R.Sánchez-Reillo, A.González-Marcos. Access control system with hand geometry verification and smart cards. Proc.33rd Annual 1999 Internacional Carnahan Conference on Security Technology. Madrid, 5-7 Octubre, 1999.

[R.Sb] R.Sánchez-Reillo,C.Sánchez-Ávila, A.González-Marcos. Multiresolution analysis and geometric measure for biometric identification. Secure Networing-CQRE[Secure]'99. Noviembre/Diciembre, 1999.

[SC78] Hiroaki Sakoe and Seibi Chiba. Dynamic programming algorithm optimization for spoken word recognition. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, (1):43–49, 1978.

[SRSAGM00] Raul Sanchez-Reillo, Carmen Sanchez-Avila, and Ana Gonzalez-Marcos. Biometric identification through hand geometry measurements. *IEEE Trans. Pattern Anal. Mach. Intell.*, 22(10):1168–1171, 2000.

[Y. 82] Y. Sato and K. Kogure. On-line signature verification based on shape, motion, and writing pressure, 1982. IEEE Proc. Sixth Int'l Conf. on Pattern Recognition, 1982.